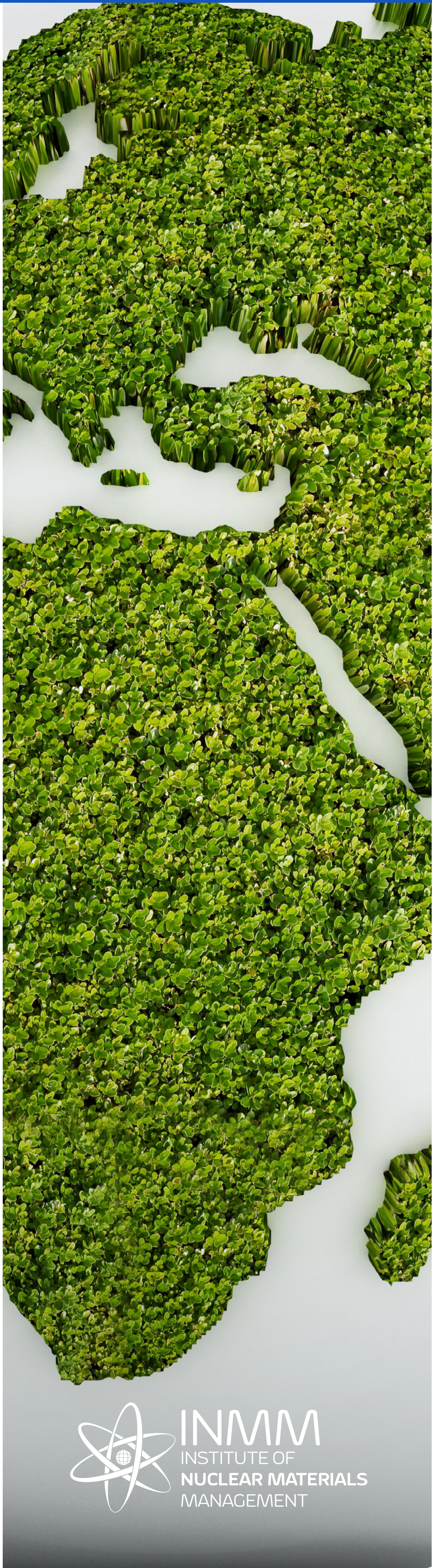
Volume XLVI, Number 4

JNMM Journal of Nuclear Materials Management



INMM
INSTITUTE OF
NUCLEAR MATERIALS
MANAGEMENT

JNMM Journal of Nuclear Materials Management

Technical Editor
Markku Koskelo
Assistant Technical Editor
Brian Boyer
Technical Editor Emeritus
Dennis Mangan
Associate Editors
Sarah Frazar, Education and Training
Alicia Swift,
Facilities Operations
Irmgard Niemeyer and Carrie
Mathews, International Safeguards
Louise Worrall and Rian Bahran,
Materials Control and Accountability
Leslie Fishbone, Nonproliferation
and Arms Control
Felicia Durán, Nuclear Security and
Physical Protection
Glenn Abramczyk, Packaging,
Transportation and Disposition
Book Review Editor
Mark L. Maiello
INMM Executive Committee
Cary Crawford, President
Susan Pepper, Vice President
Chris Pickett, Secretary
Robert U. Curl, Treasurer
Corey Hinderstein, Immediate Past President
Members At Large
Michael Baker
Kerry Dunn
Willem Janssens
Teri Leffers
Advertising Contact
1120 Route 73, Suite 200
Mt. Laurel, NJ 08054 USA
Phone:+1-856-380-6813
Fax: +1-856-439-0525
Email: inmm@inmm.org

JNMM (ISSN 0893-6188) is published four times a year by the Institute of Nuclear Materials Management Inc. The Institute of Nuclear Materials Management (INMM) is an international professional society dedicated to development and promulgation of practices for the safe, secure and effective stewardship of nuclear materials through the advancement of scientific knowledge, technical skills, policy dialogue, and enhancement of professional capabilities.

DIGITAL SUBSCRIPTION RATES: Annual (United States, Canada, and Mexico) $200 for individuals. Institutional subscriptions are $600 per year. Single copy of the proceedings of the Annual Meeting (United States and other countries) $200. Send subscription requests to *JNMM*, 1120 Route 73, Suite 200, Mt. Laurel, NJ 08054 USA. Make checks payable to INMM.

DISTRIBUTION and delivery inquiries should be directed to *JNMM*, 1120 Route 73, Suite 200, Mt. Laurel, NJ 08054 USA, or contact INMM Headquarters at +1-856-380-6813; fax, +1-856-439-0525; or email, inmm@inmm.org.

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

© 2018 Institute of Nuclear Materials Management

JNMM Journal of Nuclear Materials Management

Topical Papers

Institute News

Annual Meeting

Departments

Mission Statement

The Institute of Nuclear Materials Management is dedicated to the safe, secure and effective stewardship of nuclear materials and related technologies through the advancement of scientific knowledge, technical skills, policy dialogue, professional capabilities, and best practices.

INMM
INSTITUTE OF
NUCLEAR MATERIALS
MANAGEMENT

President's Message

By Cary Crawford
INMM President

INMM Community,

I'd like to welcome you to another edition of the *Journal for Nuclear Materials Management*. I'm writing this note on the plane from my return trip from the 2018 International Safeguards Symposium at the IAEA. The event was well-organized and provided many excellent talks, side events, and collaborations. The INMM was honored to be one of the sponsoring organizations and greatly appreciates the relationship we share with the IAEA International Safeguards Department.

At the event, we were able to reveal our participation in the Gender Champions in Nuclear Policy. As a charter member of Gender Champions in Nuclear Policy, the INMM has made the following three commitments. The INMM will:

1. Approve no slate of candidates from the Nominating Committee for any individual Executive Committee position that does not have at least one woman.
   a. Note: As the INMM is a volunteer organization, it may occur that no female volunteer can be identified. In such a case, INMM has committed to require a written report from the Nominating Committee Chair on steps taken to avoid the single-gender slate and to provide that report to all members.
2. For the technical program of the Annual Meeting:
   a. Collect data on the gender diversity of paper presenters and chairs over 2 years.
   b. Require that proposals for discussion panels or special sessions include a list of speakers that are not a single gender.
3. Develop new guidelines for session chairs at the Annual Meeting on how to achieve diverse participation in discussion/Q&A sessions by recognizing and encouraging contributions from all genders and ages in the audience, and convey this guidance in writing as part of a revised Session Chair Guide and verbally at the daily Speakers' Breakfast.

If you will recall from our strategic plan, Goal #2 was to represent the breadth of the profession, with one of the metrics being to set diversity benchmarks based on data gathering and to develop programming to address programmatic, networking, and other identified gaps to encourage participation of underrepresented groups. While diversity covers technical focus areas, international participation, gender, and other areas, the INMM believes the commitment to this initiative is a strong step in achieving our goals, and we look forward to reporting our progress in the upcoming years.

Finally, we are encouraged by the level of energy that has been given to the Institute and its future. Despite some challenges in travel to our meetings, we believe we are on the path to receiving strong visibility and support. In this edition, we will provide highlights from the 2018 Annual Meeting and look forward to future interactions, partnerships, and annual meetings. As always, should you have ideas for topics, speakers, approaches, and so on, please feel free to contact me or any of our leadership team at any time.

Sincerely,
Cary Crawford
President

The 59th Annual Meeting

By Markku Koskelo
JNMM Technical Editor

As in the past fall Issues, this issue focuses on the INMM Annual Meeting held this past July in Baltimore, Maryland, USA.

As has been our tradition for this issue, we have included the transcript of the talks made by our two plenary speakers, Dr. Maria Betti, Director of Directorate G, Nuclear Safety and Security at the European Joint Research Center (JRC) Karlsruhe, Germany, and Dr. Brent K. Park, Deputy Administrator for Defense Nuclear Nonproliferation at the U.S Department of Energy’s National Nuclear Security Administration.

The article on the plenary speeches is followed by an article on the traditional JNMM Roundtable interview of the plenary speakers. The transcript of the Roundtable includes the questions posed by the INMM leadership to the plenary speakers and offers additional candid insight from them on the intersection of nuclear science, technology, and policy with global security.

We have also included three contributed papers in this issue. The first one looks at using game theory methods and principles to guide defensive strategies for securing a nuclear facility against an attack by a highly rational and knowledgeable adversary. The second paper looks at safeguards issues in a pyroprocessing facility. The third paper looks at finding sources with an Organic Scintillator-Based Radiation Portal Monitor. This is the first place student paper winner from the 2017 annual meeting that has gone through the full peer review process. Other student paper winners are still in the review process.

Book Review Editor, Mark Maiello, provides us with a comprehensive review of the book, Insider Threats, edited by Matthew Bunn and Scott Sagan. The questions the editors ask themselves, and us, is can the insider threat experience from other, non-nuclear industries help in planning of nuclear security operations? The contention of editors Bunn and Sagan is yes. Their effort to do so is this short treatise, written with seven other experts. For anyone in the nuclear security business, a book well worth looking into.

In his column, “Taking the Long View in a Time of Great Uncertainty—New Challenges for the Institute”, Jack Jekowski, chair of the INMM Strategic Planning Committee, discusses how some of the new technological advances affect our daily work in nuclear security and safeguards.

Markku Koskelo
JNMM Technical Editor

Opening Plenary Session

INMM 59th Annual Meeting July 23, 2018

Cary Crawford:

Now I would like to introduce our distinguished speakers for this morning's session, Dr. Maria Betti and Dr. Brent Park. If they would come up and take their seats, I'll go ahead and do the formal introduction. We'll start with Dr. Betti.

Dr. Maria Betti was appointed Director of G Nuclear Safety and Security at the JRC Karlsruhe site in July of 2016. The mission of the JRC Directorate G for Nuclear Safety and Security is the implementation of the JRC Euratom Research and Training Program and the maintenance and dissemination of nuclear competencies in Europe to serve both nuclear and non-nuclear member states. JRC Directorate G supports the relevant policy DGs with independent, technical, and scientific evidence in the areas of nuclear safety, security, and safeguards.

She has also held positions as Director of the EC Joint Research Center's Institute for Transuranium Elements, the Director of the IAEA Marine Environment Laboratories, and the EC Head of Sector, Analytical Chemistry, at the Institute for Transuranium Elements. In addition, she served the Italian National Research Council and Department of Chemistry and Industrial Chemistry of the University of Pisa, Italy, where she continued to lecture until 2012.

She obtained her doctoral degree in chemistry with a specialization in environmental, instrumental, and radiochemistry from the University of Pisa in 1984. She has authored 120 publications in the field of analytical chemistry, radiochemistry, environmental/instrumental chemistry, as well as nuclear safeguards in international journals with high impact factors. She also authored several chapters in scientific books and has participated in numerous international conferences as an invited speaker.

In 2012, she was international winner of the Prix Monte Carlo Femme de l'Année for the establishment after the Rio+20 summit in the International Center on Ocean Acidification at the IAEA office in the Principality of Monaco. From 2004 to 2008, she chaired the JRC Women in Science Network. Most recently, in 2016, Dr. Betti was honored with the Magnificent Distinction by the Ordre de Saint-Charles.

Dr. Betti, the floor is yours.

Maria Betti:

Distinguished guests, ladies and gentlemen, it is an honor and pleasure for me to be here today to open the plenary of this 59th Annual Meeting of the Institute of Nuclear Materials Management, the organization aiming at being the leading international professional society for the stewardship of nuclear materials and related technologies to enhance global security. I would also like to warmly congratulate the INMM on its 60th anniversary, which makes this Annual Meeting even more special. The rising interest in using nuclear power for civil purposes in a number of new areas on the globe makes meetings like the one we have the privilege to attend today a very valuable opportunity for many professionals (with a variety of backgrounds and insights) to meet and discuss both the latest developments and the many challenges that still lie ahead. I sincerely believe that it is mainly thanks to the value-added exchanges that such a high-level, wide forum enables that together we can reach our common goal to advance and secure the future of nuclear materials management, which remains — even more today than 60 years ago when INMM was created — a truly international endeavor.

Being devoted to ensuring the safe, secure, and effective management of nuclear materials and related technologies through the advancement of scientific knowledge, technical skills, policy dialogue, professional capabilities, and best practices, the mission of the Institute of Nuclear Materials Management is particularly relevant to the overall mandate of the JRC — which I represent here today.

As the European Commission's science and knowledge service, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle. Its work has a direct impact on the lives of citizens by contributing with its research outcomes to a healthy and safe environment, secure energy supplies, sustainable mobility, and consumer health and safety.

While most of our scientific work serves the policy of the Directorates-General of the European Commission, we address key societal challenges while stimulating innovation and developing new methods, tools, and standards and by taking advantage of our long-standing scientific expertise, modeling capacity, foresight studies, and work on standards, infrastructure, and e-infrastructures. We continuously share know-how with the member states, scientific community, and international partners.

In the new organization of the JRC, entered into force on July 1, 2016, the continuous effort in reinforcing and broadening the JRC nuclear skills attained a greater consistency, while increasing our Directorate-General leadership and impact in Europe and worldwide as the reference center within the European Commission for Science and Knowledge.

Following the validation of a new strategy, the JRC Directorate G for Nuclear Safety and Security — which I have the honor to lead as director — has gathered the totality of the JRC's nuclear work, funded by the Euratom Research and Training Programme, and in this frame keeps as key objective the pursuit of research, knowledge management, and training activities, with an emphasis on nuclear safety and security toward the maintenance and dissemination of nuclear competences in Europe, to serve both nuclear and non-nuclear member states. Thus, we contribute to the transition to a carbon-free economy in a safe, efficient, and secure way.

The JRC is also an active key partner in international networks and collaborates with international organizations and prominent academia and research institutes. A strong cooperation and complementarity with member states' national organizations continues to be relevant to our work.

The JRC aims to become a central point in the Commission for information and knowledge in support of the development and implementation of nuclear safety, security, safeguards, and radiation protection EU policies.

To this extent, our collaboration with the INMM proves to be extremely significant. The strength of INMM in my opinion does not only lie in its institutional memory and the technical competence and experience of its members, but also in the national and international network that INMM operates and continues to expand, based on the creation of and interaction with a large number of subgroups of interested colleagues, at both regional and national levels.

In these times of occasionally strained political relations involving a variety of international partners, the continuous effort in keeping the dialogue open between professionals, scientists, and — where possible — authorities is deemed of crucial importance.

In this context, I would like to acknowledge the JRC's active contribution, during a number of years, to the INMM by initiating and maintaining interactions with a variety of these Chapters through the Chair function of the Chapter Relations Committee.

The very positive outcomes of our collaboration to date confirm the JRC's intention to keep supporting the outreach of the INMM in the future.

One way in which we implement this is through the key role that JRC is playing in the leadership, organization, and working groups of ESARDA (The European Safeguards Research and Development Association), with whom INMM recently signed a Memorandum of Understanding. I am particularly pleased that this collaboration has been intensified strongly in the last years.

Whereas in our last open ESARDA Symposium in Dusseldorf — organized by ESARDA president Irmgard Niemeyer, from Juelich — we had about 40 U.S. participants (apart from other international contributors), I would like to encourage all of you here today to mark in your calendar the next open ESARDA Symposium, which will coincide with the 50th birthday of ESARDA. That is organized by the future ESARDA president, Willem Janssen from JRC, taking place from May 14 to 16, 2019, in Stresa, on the Lago Maggiore, in the north of Italy.

Providing an expertise-based discussion forum such as this Annual Meeting is fundamental first of all in the area of international nuclear safeguards, as the current discussions over and status of the Joint Comprehensive Plan of Action for Iran show. A number of new and proven techniques continue to be deployed by the international inspectors in Iran, and they are enhanced by additional and unique tools (such as the procurement channel). The IAEA plays a crucial role in the overall verification protocol.

The fact that it was recognized, while negotiating this deal, that beyond the nuclear materials themselves, the technology, components, and knowledge also matter, was in my opinion already a major success for the nonproliferation regime itself.

The results of the nuclear verifications are regularly reported by IAEA to its Board Of Governors (BOG), and this is also the basis for the stable relations that especially the EC and some other international partners strive to maintain with Iran. With respect to the overall international safeguards approach and implementation, we expect to hear a lot about the latest evolution and current challenges during the upcoming IAEA nuclear safeguards symposium in early November 2018 in Vienna.

Without anticipating the outcome, I expect — and would certainly hope — that the discussions and contributions from the specialists in nuclear safeguards and nonproliferation will lead to a further strengthening of the state-level approach and the integrated manner in which IAEA currently develops its safeguards reports.

I deem the developments achieved in the last years in this respect by the IAEA — often supported with very valuable contributions from the various support programs to the IAEA in the area of safeguards — as very encouraging to further enhance the safeguards conclusions on the one hand and to assure a nondiscriminatory and efficient approach towards the country verifications on the other, in line with their respective safeguards agreements.

In the nonproliferation area, the even more visible event in the form of the June 12th summit in Singapore between the U.S./North Korea confirms that risk of proliferation of nuclear materials, technologies, know-how, and conversion into nuclear weapons, and determines the world political scene. This also constitutes a key challenge to INMM as an organization and to its members and partners.

In fact, they can make a major contribution to the recognition of the risks, the quantification of specific indicators, or the development and testing of tools for monitoring remotely specific sites or activities. Even if no verification regime for potential disarmament has yet been discussed or analyzed, it goes without saying that this international community of nuclear professionals will be challenged to provide the most efficient and effective tools for such purposes.

It might be premature — but, on the other hand, also pertinent — to refer in this respect to the International Partnership for Nuclear Disarmament Verification (IPNDV), which in its first couple of years of existence — especially during Phase 1 of the initiative — has put the focus on available technologies and approaches for verifiable disarmament. I know that some Technical Divisions from INMM follow these developments closely, and also in my organization we have been hosting the Working Group 3 (focusing on the technology), and it turned out that a substantial amount of the proposed technologies rely on the developments and experience gained in nuclear safeguards applications in civil facilities.

As of today it is not yet clear which role can be played in this respect by international organizations, but IAEA has set up a dedicated task force available to start the verifications in North Korea (and reconstructing the chain of knowledge) if so tasked by the IAEA BOG.

Ladies and gentlemen, let me highlight the specific role that our organization is playing in this broad context. The Joint Research Centre continues to conduct research and to provide technology, instruments, technical services, sample analysis, and training for nuclear safeguards, including the verification of treaties and agreements, to inspection agencies, states, and operators, as planned under the Euratom treaty and in support to IAEA. The JRC will continue to strive for enhanced efficiency and effectiveness of current safeguards approaches, tools, and methodologies. This applies in particular to the field of improvements of techniques for nondestructive analysis, destructive analysis, particle analysis, process monitoring, enhanced verification technologies, advanced sealing technologies, nonproliferation studies, and strategic trade control, while at the same time providing substantial support in training activities to both DG ENER and IAEA inspectorates.

In the area of nuclear security, a close collaboration exists also here between the JRC and the IAEA, and although we recognize that nuclear security is in the first instance a member state responsibility, there are definitely a number of fields where an international professional organization can contribute (such as validation, testing of equipment, standardization exercises, benchmarking of methodological approaches). The INMM's own work, through its technical division — for example, on physical protection and cybersecurity — are worth mentioning in this area. In Europe, we provide scientific and technical support to nuclear security both under the "Internal EU Action Plan, funded by DG HOME" and the "External Peace and Stability Action Plan" (mainly known under the name Centres of Excellence), funded by DG DEVCO.

The particular characteristic of these latter two action plans is that they do not address nuclear in isolation but in fact try to cover the whole spectrum of WMD threats (including chemical, biological, radiological, nuclear, and explosives).

Still in nuclear security, we appreciate the strong collaboration between INMM and WINS (and a speaker after the coffee break will highlight some key results of this) and the transatlantic collaborations, such as the one between a variety of U.S. national laboratories and European Commission laboratories (and, of course, also EU member states laboratories).

In fact, it turns out that just 2 weeks ago in our research center location in Ispra, Italy, we had our annual review meeting of the collaboration between Euratom and the U.S. DOE (and other U.S. Departments), which is a very productive and fruitful collaboration mechanism, covering the areas of nuclear safeguards, nonproliferation (including strategic trade control issues), and nuclear security. Dave Huizenga, Principal Assistant Deputy Administrator for Defense Nuclear Nonproliferation at the National Nuclear Security Administration, led the U.S. delegation, which, after a quite detailed visit to our laboratories, made plans to further enhance our collaboration in the future to the benefit of the international society and especially also to IAEA.

Still in the area of international collaboration, last week, also in Ispra, we met with the colleagues of the Border Monitoring Working Group, an international coordination mechanism in the area of enhancing nuclear security (detection, response, on-site assistance, training, etc.) at crucial transport nodal points, and which was set up 20 years ago (largely out of necessity to assure the compatibility and synergies between different international providers of in-field support), and which includes the U.S., EU, and IAEA.

Another very important characteristic of INMM — particularly significant and in line with the mandate and activities conducted by the JRC — is its strong outreach to university students and young professionals worldwide, especially through the so-called Student Chapters (currently 25 exist worldwide).

This investment in the education, training, and knowledge transfer to the younger generation is crucial in our field of advanced nuclear technology, where many experiments were done and knowledge gathered more than 50 years ago — which means that that knowledge was gathered by a generation that has now largely finished their professional career and is thus no longer available for on-the-job coaching and teaching of younger staff. The fact that the number of universities teaching nuclear technology is certainly not increasing and that the amount of nuclear experimental facilities has significantly reduced in the last decennia underlines even more the importance of networking, sharing facilities, and student exchange. In our JRC facilities back in Europe, for instance, we strive to provide as much as possible open access to our highly specialized research infrastructure and thus operate as a user facility for European and international stakeholders.

Knowledge management has also become in recent years a key topic of JRC interest and action. Knowledge management has become a priority for the JRC, as demonstrated by our new structure and organization entered into force on July 1, 2016. While creating new knowledge will remain the JRC's core function, the new vision refers to "managing and making sense of collective scientific knowledge for better EU policies. This means, inter alia, collating and analyzing it and communicating it to policymakers, in a systematic and digestible manner from a source they trust." The reflection paper on data, information, and knowledge management at the Commission has led to the development of science-based Knowledge Centres (KCs) and Competence Centres (CCs) in priority policy areas where policy needs to be supported by scientific evidence. KCs will create, collate, validate, structure, put into context, and make comparable, easily comprehensible, and accessible internal and external scientific knowledge for a specific policy field or across policy fields. CCs will bring together analytical expertise, such as modeling or data mining, which is independent of theme and can be applied across policy areas.

A Knowledge Centre on Strategic Trade Control is currently under discussion at the JRC management level, as it has been identified as a key priority and field where JRC has demonstrated substantial expertise and support to the policy DGs in this cross-discipline area. Strategic trade control is considered as a central contributor to the nonproliferation regime, and further international collaboration in this field is thus very welcome.

As an example of an efficient knowledge management system and network, ESARDA confirms its central role in contributing to strengthening nuclear safeguards programs and policies at the international level, most of all in contributing to a resilient knowledge management strategy on nuclear issues.

Ladies and gentlemen, I would like to close by conveying to this notable audience a message of encouragement by underlining once more the importance of actively participating in and supporting the INMM and of the added value of being part of a highly professional society promoting dialogue and exchange of good practices toward the safe stewardship of nuclear materials and related technologies, for the sake of global security. While renewing my gratitude for having invited me to open this 59th Annual Meeting, I wish the INMM much success with its ambitious objectives and current work, and to all of you a very successful participation and pleasant continuation. Thank you.

Cary Crawford:

Thank you very much, Dr. Betti. We very much appreciate your talk and your remarks toward the Institute. We will take you up on the offer on how to better collaborate.

Our next speaker is Dr. Brent K. Park. Dr. Park serves as the Department of Energy's National Nuclear Security Administration Deputy Administrator for Defense Nuclear Nonproliferation. He's a nuclear physicist with extensive experience in congressional and executive branch interactions. Dr. Park collaborates with and advises representatives of the U.S. National Defense, Homeland Security, and Intelligence Communities in the application of advanced technologies to fulfill national security missions.

Prior to his current assignment, Dr. Park served an associate lab director at Oak Ridge National Laboratory, leading the science-to-application efforts for the laboratory's national security programs. He was responsible for DOE/NNSA programs at ORNL.

Before joining ORNL, he was the director of the DOE/Non Steroidal Anti Inflamatory Drugs Remote Sensing Lab, where he led efforts to advance and field cutting-edge diagnostics and communication instruments in support of counterterrorism and radiological incident response for the nation. Earlier, he managed and contributed to basic and applied research programs at Los Alamos National Laboratory in the areas of defense nuclear nonproliferation, nuclear emergency search team activities, modeling and analysis for nuclear weapons engineering efforts in support of stockpile stewardship, nuclear weapons physics, and basic physics research.

Dr. Park earned a bachelor's degree in physics and mathematics from Illinois State University and a master's degree in physics with an emphasis on remote sensing at Indiana State University. Later, he shifted the direction of his research to nuclear physics and earned a second master's degree at Indiana University. He performed his thesis experiment using the spallation neutron source at LANL and earned a doctorate in physics from Ohio University. Please welcome Dr. Park.

Brent Park:

Good morning.

Audience:

Good morning.

Brent Park:

While I was going through the confirmation process, Teressa McKinney, my staff, asked me if I could come and talk to a few people. Hello, a few people. Anyway, without thinking, "Oh, sure, I'll come over and talk to you." I didn't realize there were so many few people in this room.

I spent the last few days asking my staff — in fact, a couple are here — "What should I talk about?" They gave me great ideas. I didn't like any of it. In fact, they looked like what you can find on the DOE/NNSA website. I've been asking, starting with Teressa, Larry, everybody, Corey, everybody, "What should I talk about?" This is my parking ticket. By the way, you guys owe me $45.

I actually collected keywords. I'm going to make things up along the way. Since I've been doing this for about 30 years, I should be able to entertain you on three topics. I'm going after great speakers, so you can actually check off a few things. Along the way, every 5 minutes, I was just checking off, "Okay, there it goes. There it goes."

The last couple of things that remain for me to entertain are R&D, obviously — I'm a physicist, so I'm going to talk about that a little bit. Then, education. Again, as the previous speakers said, it's great to see many universities participating. I will actually focus a little bit on the students and young postdocs. I was one many years ago. In fact, that's how I started my career in Los Alamos National Lab.

But I'd like to actually congratulate Morris. It's good to see your friend becoming a fellow, by the way. It's a good deal for one of my NNSA fellows to — or, a coworker to be a fellow here at INMM. That's a great recognition for Morris.

Anyway, let's see, R&D. Much of what we do is science and technology-based, by the way. We call it science, but, in reality, it's science, technology, engineering, and everything else you can throw in. That's what we do, by the way.

When I actually first got to NNSA headquarters a few months ago, one of the things I found very surprising and interesting is the people. I knew them from a distance for about 30 years. I worked with them, partnered with them, but again, I didn't realize the amount of work that they've been doing. In fact, it's good to see many of my office staff here rather than at my office, by the way. It's great to see you here.

But, again, that also worries me quite a bit, because many of the people are old enough to retire. I'm going to tiptoe around and I'm going to give you some discrete talking points. I'm going to pull them all together toward the end.

As it turns out, when I was going through a confirmation process at the Senate, many senators actually asked me, "Dr. Park, one of your 'sales pitches' is to nurture the next generation. How are you going to do that?" I went through the normal routine of education, university outreach program, and so forth.

But, again, many senators pointed out that we have to compete against Googles all over the world and so on. It's not that easy. One draw that we have is mission. Many of you and many of your colleagues believe in the mission space that we're in, national, international security, and peaceful coexistence, and so on. That's a big deal, by the way. One of the institutes or societies that I've been meaning to come by is actually this Institute, because it's important for me to engage with you and emphasize how important it is that we work together.

I actually had a closed-door conversation with my staff a couple of weeks ago, maybe it was a week ago. They asked me about my vision for NNSA and so on and so forth. Those secrets are kept in the government, by the way, because as soon as I said I'm going to emphasize the R&D, guess what? Everybody in the hallway tells me, "Oh, Brent, you're going to grow our R&D program to whatever it is."

Yes, that's true, actually. That's the part that we have to focus on. The words that I use are intentional, and we need to focus. It cannot be done by excellence. You have to have desire and a plan and support and the willingness to do all of this. Again, special thanks to — there was an award winner who actually thanked this professor. It starts with education, by the way. That's a big deal. Much of what we do for treaty verification, monitoring, and so on and so forth that my office is responsible for — it starts with education.

In fact, we actually have three relatively large university consortia. I think that there are three — Berkeley is the leading one, Michigan, and North Carolina. One is about to go for a recompete. But, again, through these programs, we actually engage with you, work with you, because we actually put national labs to work with these university centers, so we can maximize the impact.

The focus, number one, is people: students, early careers, as well as professors. You need to stay engaged, and we've got to make these opportunities available. In fact, the Administrator for NNSA, Lisa Gordon-Hagerty, and I agree that we need to invest more. Hopefully, over the next 6 to 12 months, we'll actually announce more interesting opportunities. Stay tuned for that.

Locally, we also have this fellows program within NNSA. It started long before. In fact, it was out of what is now my office, but it got broadened, and we actually include other parts of NNSA. In fact, if I remember a statistics in — I ask my people to give me numbers, and I don't remember exactly what they are. They told me about a hundred times, but roughly about 450 people graduated from this fellows program. It's about a year-long program. Our placement percentage, if I can call it that, is 98% or 99%. In fact, many of my senior staff, there are some Senior Executive Service staff in my organization who are graduates from this fellows program.

We're looking at all different aspects of giving opportunities to early careers. In fact, when I was a postdoc in Los Alamos National Lab many, many, many years ago, somebody took pity on me and gave me a job in the Physics Department. That's how things worked. It is important that we continue the tradition. Thirty years later, who would have thought that I'd be here talking to you? By the way, this parking permit, I cannot lose.

One thing that I've been struggling whether to actually discuss or not is civilian nuclear energy. I'll just say a few words and get off and take your questions. My office is responsible for what we call 123 agreements and expert control license agreement, overuse, and so on. We really need to make sure that, starting with the United States, our partners and allies and everybody in the international community applies nuclear energy for peaceful purposes.

It sounds simple, but much of the technologies that go in to making sure that they're used peacefully — I'm looking at the people who have to make that happen. We need great ideas. In fact, I was very happy to hear that there is a renewed emphasis on modeling and simulation, because you cannot actually perform all the experiments that you can think of, really. You have to rely on the latest and the greatest modeling and simulation tools. In fact, I'm very happy to share with you that my former organization, Oak

Ridge National Lab, reclaimed the number one. It's called the summit, I believe.

But, again, it's a great competition for all of us: nations competing on science and technology. That's what I'd like to see personally, all the societies and institutes like this. You compete for recognition. That's how we need to actually compete with each other, and that's what to look for.

A few weeks ago, I made a first official travel to Vienna, just to say hello to my colleagues at IAEA and CTBTO. Relationships are important, as the previous speaker actually talked about. You actually have to build them when you don't need them.

For the young people, it's critical that you convince your professors and your supervisors to attend these important gatherings. In fact, I actually encourage all my fellows to find time to participate in these important meetings. Many of my staff I see in the audience, and many of my former lab colleagues are in the audience. In fact, I've been supporting Larry Satkowiak and Teressa and everybody else, and I didn't realize I was missing this kind of fun. Had I known, I would've been here a long time ago.

I could go on and on, but the important thing here is that I appreciate all your dedication and active participation in educating and training the next generation. In fact, many of us are at an age where we actually have to worry about who's going to fill our shoes and fill our jobs and so on so forth. It's critical. That goes to our international partners as well.

But, again, if you take away anything from my talk this morning, a very brief one, is that thank you for all you've been doing. Although there isn't a whole lot of R&D in nuclear nonproliferation, by the way, it's built on R&D, it's built on S&T, it's built on technical people like yourselves. I cannot ignore the operation and support people, RCTs included, and so on and so forth, that they make our jobs more effective and livable, if I can use that word.

But, again, it's a team effort, team concept. As a dumb physicist in a palace job, I'm learning every day. It's eye-opening. But, again, I look forward to applying my R&D, S&T background. The next time you invite me, I'll talk about something like how this "palace thing" is working out for a dumb physicist like me, but for now thank you. Good to see you.

Cary Crawford:

Thank You, Dr. Park. I will take this opportunity now to allow you to ask some questions of either Dr. Park or Dr. Betti. I would remind you that we have mics in the middle. Okay. If you do have questions, please step up to the mics in the middle.

One comment I didn't make at the beginning, just for your awareness, in case it matters to you, this is being live streamed. If you have a question that you don't want your boss to hear, maybe you'd think twice about it. But, otherwise, we would very much welcome questions. We have a few minutes for that. Anybody who wants to ask questions of either speaker? I see one working his way over.

Nickolas Roth:

My name is Nick Roth. I work at Harvard University. My question is for Dr. Park. Over the last few years, there's been a decline in budgets for international nuclear security programs within NNSA. I want to ask you what do you think your approach will be so that innovation in that space and encouraging new ideas?

Brent Park:

I appreciate the question. It's so blindingly bright, I cannot even see your face. If you move this TV, by the way. For the organizers, you need to entertain short people like me. The legs … It's far back. I've got to find a way to make you laugh once or twice this morning because, otherwise, I would not have succeeded.

A very good question. As it turns out, everything is cyclical in what we do. It's not so much the lack of funding, by the way. Many things that we have started we've successfully concluded. We've been collecting and reviewing new strategies, which is the second part of your question, what we're doing and so on and so forth.

It's not done in a vacuum, it's done with international partners and it's done with the lab sites and plants and university colleagues and so on. Part of my job is to make sure that we build the next 3- to 5- to 10-year strategy. I'm happy to share with you that whatever we're doing that is in part of a 2020 budget cycle looks promising. Obviously, we cannot go into details because it's still embargoed.

But, again, we're very hopeful that whatever we have been doing will be sustained and that we'll put some new emphasis on new projects and new programs. That's what we're going to be doing. Thanks for your question.

Edwin Lyman:

Yes, Dr. Park, this is Ed Lyman from the Union of Concerned Scientists. I hope you don't mind if I raise an issue that you didn't talk about and probably don't want to talk about.

Brent Park:

Good to see you again.

Ed Lyman:

First, a comment about the disposition of surplus weapons plutonium. I just wanted to say that we appreciate that the Administration is continuing to pursue the termination of the MOX program and the dilute-and-dispose alternative. We're very supportive of your efforts to maintain your policy in the face of congressional opposition. We stand ready to support you in any way we can on that.

But on a related note, in a report to Congress in June, NNSA said — as you know, you're under a court order to remove one metric ton of plutonium from South Carolina by the end of next year. You told Congress that you were considering repurposing some or all of that material for defense purposes.

The question that I'm asking you, which you're not going to want to answer at this point, is does that mean that you're actually considering withdrawing up to one ton of material that's currently designated surplus plutonium, withdrawing that from the excess stockpile and returning it to the weapons stockpile? Because we would be concerned about the development. We're wondering why that decision is being considered. Thank you.

Brent Park:

I don't think he expected an answer from me. Well, we review all options, obviously, and we take seriously the court orders, as well as we are trying to find ways to partner with the friends in South Carolina and elsewhere. We're hopeful that several options we're entertaining will lead us to successful conclusion. Again, there are things that I'm not at liberty to talk about, but, again, we're looking at all options diligently.

Cary Crawford:

Other questions? I'm seeing none coming. I would like to tag on both of your comments and more from the INMM perspective, but I very much appreciated your comments about the interactions between not only the institutions represented here but many others. Each one seems to have a different focus and a different mission.

One thing at the INMM that we like, which we haven't seen as much of in recent years, is with such an august group of scientists, engineers, policy, technical people, implementers in facilities, we like challenges. I don't think we have been as good about standing up in front of the Institute and presenting big challenges, but we do historically have a history in having accepted challenges and achieved those challenges. We'll speak about one example in just a minute.

I very much appreciate your comments about the interface. I guess I would challenge you and the Institute to think about how we might be able to help you further your missions in better in achieving your goals in all of the different fields of nuclear materials management.

Bruce Moran:

Bruce Moran, Y-12. Both of you represent research and development in science and the technology development. A lot of us out here are involved in the implementation as inspectors, as operators. How do you see that the interactions between research and development and those using the products of your research and development?

Maria Betti:

Personally, I see that in research and development, we need to look at the gaps so that we are in the technologies. In looking at these gaps, we have to see how the answer can respond to some questions that the inspectors of those that are using this technology are looking for, namely if there is a new request or new need for verification, for instance, from Euratom inspectors, and they want to have a particular case to develop, they can come to us and discuss with us. I have a practical example.

Look at the remote control that we are developing for some repository like that in Finland. We have worked with the nuclear inspectors to understand the best to verify the waste ones in the repository. We have developed a 3D system of remote monitoring that actually can be used not only for this purpose, but also for some others that nobody would believe, like the reconstruction of cultural heritage.

This is how I think, and some implementation of techniques should go with research and development. They have to work together. The researcher, who is in research and development, has to respond to technological gaps, but the technological gaps have to come out from those who are doing the implementation.

Brent Park:

I was in Vienna a few weeks ago. I visited with the IAEA and CTBTO. They actually zoomed in on one aspect of instruments, technologies, and so on and so forth, which is immature. Is it ready to use by just about anybody? As it turns out, most of what we do at university and the national labs is cutting-edge. Oftentimes they are not ready for field action. There's a little homework on our side, by the way.

Not everything is usable. The biggest example that people use often is OLEM, Online Enrichment Monitoring. If you actually open it up, it's simple technology, a collection of technologies, by the way. It's got a pressure monitor, radiation detectors, and so on, and it's tamper proof and all that.

But, again, we need to challenge ourselves into converting or maturing the cutting-edge instruments to be more field-deployable, by the way. It needs to be "uniform," so anybody can use it and get the same result.

But take everything out for a second. Much of what we do is actually how we do what we do, so the people aspect is very, very important. It's more than instruments — it's training people to do it the right way. It's a combination, by the way.

We can spend the whole day talking about the answer to the question, but that actually is one of the objectives that we have. How do we empower the people out in the field, whether inspectors or responders or colleagues, to actually have the latest and the greatest, but at the same knowing that there's a "price limit" — i.e., if they cannot afford it, what good is it? We need to understand all aspects of what it means to develop a set of technologies for field use and so on and so forth. But, again, this is a very important topic. It's worth a conversation.

Laura Holgate:

Yes, good morning. Laura Holgate from the Nuclear Threat Initiative. Thanks to both the speakers for your contributions over your careers and for your remarks this morning. Thank you, Cary, for mentioning the panel discussion that I'll be leading on Tuesday afternoon on advanced reactors and how they relate to safeguards by design and security by design.

One of the missions to my madness is to try to draw the advanced reactor community more closely in with the INMM, because I think there's technical aspects across the INMM mission space that affect these new types of reactors, whether it's high-temperature gas, molten salt, liquid metal. I'd really like to ask you two in your respective roles as technologists — and Dr. Park, especially you in your policy role — how are your organizations engaging with the advanced reactor community? How are you thinking about developing new models of safeguards and security that are associated with these new technologies and the challenges and opportunities that they'll be bringing us?

Brent Park:

Thank you, ambassador. Appreciate it. A bit of a role that we play in the fast reactors, test reactors, and so on and so forth is how we supply the fuel. For example, there is a recent conversation on the community needing high assay LEU. As it turns out, within the U.S., there is no current capability. Could we do it? Sure, but right now we don't have a capacity to do it, capability to do it.

We're helping out on the conversation to make sure it's done using S3: safe, secure, safeguards conditions are all met and so on. As it turns out, it's easier said than done, but what I offered to my colleagues at the White House and working with the nuclear energy and other partners throughout is that we want to get involved at the early stage so we don't apply brakes halfway into the development cycle. The things we can do upfront, we'll do it.

It's a simple procedural change, but, again, what I offered is, "let us take a look early and let us help you to achieve the end state quickly." This administration is really all in on getting the nuclear energy up and running again. We want to do everything possible.

Again, our job is not to apply brakes, our job is to make sure safeguards conditions are met. But, again, historically, we've been at the tail end of it. People would bring us solutions and we'd say, "No, it wouldn't work." "No, you've got to do it different."

But, again, slight change in this administration, which is very, very important, is we're taking a look at it now at the early stage, at the design stage. Over the next month or two or three, I think my office will get finally some of the designs for early reactors, different kinds and so on, rather than waiting for a year or two. Obviously, we have to sign a nondisclosure agreement and all that.

But, again, we are the U.S. government, and we will protect the information and all that. But we're looking at assisting, partnering with the industries upfront early. We're looking for all possible ways to make things happen.

Maria Betti:

Okay. Thank you very much. As you know, in Europe, for the moment, we've been mostly involved with the safety of the new reactor, the advanced reactor, namely these are generation four with the different six types.

In our work program of my directorate,

2 years ago, we already started to have a project looking at the holistic approach of these advanced reactors, also for the modular reactors, from looking at the safety aspects but also the safeguards and nonproliferation aspects. These are in collaboration with the Euratom, of course, directorate, but also with those member states. We are doing the technical developments of the reactor itself.

Laura Holgate:

Thank you.

Junichi Ishihara:

My name is Junichi Ishihara with JNFL. I have a simple, but difficult, question for Dr. Park. JNFL has been preceding the JMOX project in combination with the Rokkasho Reprocessing Plant. I used to take responsibility of the head of the General's Project for 5 years. Two years ago, I visited MFFF .... I have a question for you. Is there any possibility to restart the construction of MFFF?

Brent Park:

The MOX facility, or MOX project as we call it — the administration has declared its intent and proposed the solution. Again, there isn't a whole lot that I can add to the conversation. But, again, to the extent that we can share information and so on, I'll be more than happy to work with you and your colleagues to see if there's a lesson learned and/or if there are ways to cooperate, collaborate. We'll look for all options and avenues. But, again, the Administration has spoken, and there isn't a whole lot that I can add to the topic.

Junichi Ishihara:

Thank you.

Brent Park:

I sound like a politician, by the way.

Cary Crawford:

Any other questions? Okay. Again, I would like to thank both of our speakers. Let's give them a round of applause.

JNMM Roundtable

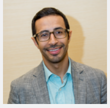
Opening Plenary Speakers

Maria Betti
Director, EC G Nuclear Safety and Security, and
JRC Karlsruhe Site

Brent Park
Deputy Administrator, DOE/NNSA Defense
Nuclear Nonproliferation

JNMM Editorial Board Participants

Glenn Abramczyk
Packaging, Transportation and Disposition



Rian Bahran
Materials Control & Accountability

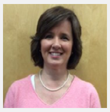
Cary Crawford
INMM President

Robert Curl
INMM Treasurer

Felicia Duran
Nuclear Security and Physical Protection

Corey Hinderstein
Immediate Past President

Jack Jekowski
Taking the Long View Editor



Teressa McKinney
Technical Program Committee Chair

Irmgard Niemeyer
International Safeguards

Chris Pickett
INMM Secretary

Larry Satkowiak
INMM Past President

Alicia Swift
Facility Operations

As it has for two decades, the *Journal of Nuclear Materials Management* hosted a roundtable discussion with the opening plenary speakers at the INMM 59th Annual Meeting. The participants had an opportunity to ask the plenary speakers questions based on their presentations during the opening session.

Larry Satkowiak: During the opening plenary, both of you described your organizations somewhat. And the perception that I get regarding both organizations is that both of the organizations work in that space between policy and technology. And I guess my question is, what do you consider your greatest challenge in that space? Is it technology? Is it policy? Is it a combination of both? And how do you manage that?

Maria Betti: So, thank you very much. Before I answer, or I try to answer your question, I would like to say a bit more about the recent reorganization of the nuclear activity inside the JRC entered into force in 2016, under the Juncker Commission. The Joint Research Centre is the General Directorate providing the scientific evidence and knowledge to support other DGs in policymaking. The JRC leads nuclear activities over four different geographical sites that could be compared to the national laboratory CR in the States. These activities started after the signature of the Euratom Treaty, the Rome Treaty in ‘57. When the JRC opened its doors, we had nuclear and non-nuclear activities conducted over four different sites. So, in 2016, the JRC endorsed a new structure reuniting its nuclear mandate under one single Director — instead of four — responsible for the execution of the JRC mandate under the Euratom Treaty.

This optimized structure constitutes the most consistent approach to respond to policy requests and to our policy-support responsibility, to be implemented at units’ level. This was one of the major results achieved by the newly appointed commission of President Juncker, which was willing to break silos at policy level inside the organization in an attempt to modernize and make it more efficient. This means an increased collaboration between different portfolios and the technical support services, which has been successfully implemented thanks to the JRC’s new structure entered into force in 2016.

Now, coming to your question and taking into account these circumstances, there is a constant need to translate policy into technology and technology into policy — how to meet politicians’ needs and address the way they express these needs. How can scientists and technicians better respond to politicians’ demands, to provide them with an effective policy support and produce scientific evidences fit for purpose? How can we communicate together? In these questions lies the challenge.

If I would simply try to ask one of my scientists to explain something to a politician, it would prove not sufficient or not clear enough. They would enter in the technical details, and the mutual understanding would be affected by this incapacity to use a common code. So, first of all, I would approach the issue by educating with dedicated trainings on knowledge management for policy support. Pure scientists need to be put more in contact with the peculiar trends defining present politics and be able to timely and significantly contribute in reaching its strategic objectives. They need to develop their understanding of the policymaking process as to start translating their jobs and communicating results in a way that can prove truly accessible and effective — not only to policymakers, but also to the general public, because the politicians finally are elected to represent the interest of the citizens. This fine-tuning in the communication process between politics and science is something we need to tackle and positively develop in the name of more inclusive and more efficient policymaking practices, in the interest of the citizens.

Brent Park: So, to answer your question. It’s not left or right, it’s not top or bottom, it’s not push or pull from the technology to policy and vice versa. What it is is actually quite intertwined. They’re connected. Depending on what the topic is, size does vary, and sometimes we make it a little more complex, complicated than it should be. But again, my viewpoint is quite different than, “Is it this or that?” But it’s actually — when you look at it from top to bottom, it’s actually one in the same. So I like to see it as technology combining and supporting policy and vice versa, not one or the other. And I think you’ve done a really good job actually of talking about the scientists working with the politicians or policymakers and so on and so forth. But again, as a physicist, I see all possibilities, but again, it’s not one or the other. It’s actually hard to separate them, and you should not separate. It’s one supporting the other.

It could be kept on my shoulders.

Felicia Duran: Will Tobey this morning issued a new challenge, and I don’t think it’s just for INMM. It’s for all of us that work in these areas, that’s security and safeguards and related areas. [He] issued a new challenge regarding professional certification of the staff that work in these fields. And I know both of you really did emphasize the importance of education and training in your remarks this morning. So, how do you think, or given this challenge, what can your agency do to meet that challenge that WINS issued this morning?

It's actually worthwhile. And what it does is it actually puts a spotlight on one of our much-needed efforts. And to that extent, I accept it and I think all my fellow colleagues do accept the challenge. Because it's the right thing to focus on. And I use this work today when I talk about R&D and so on. And the work is intentional. They do show up in the way I actually process these challenges, by the way. So that there is a call worth our time, our while; we need to embrace it and develop a plan to make sure that we can deliver something to the committee and to the nation, and as one partnership and so on.

It's easy to say, "Yes, we take the challenge." It's quite a different matter of when you actually have to present an action plan and how we go about actually meeting those challenges head on and so on and so forth. And I think that's where a body like INMM could come into play. Keep us focused. Bring it up on a regular basis, not just at the annual meetings, but on a regular basis. And call us up to make sure we do our part.

But again, it's a partnership. It's not just people on the government side or people on the university side, people on the lab side; it's a partnership. It's a collective fight so to speak. And to that extent, we like to hear thoughts and ideas from the community as to what we should be doing. Knowing that we have constraints on the government side as to what we can and cannot do, I appreciate the good ideas. At the same time, we are riding on proven ideas. And a couple of the examples. I did talk about the Educational Center Program, which sits at the center of what we're talking about. I talked about the Fellowship Program, which is also in the center of what we're talking about.

But to an extent, how do we broaden those possibilities? It's getting more of the government saying, "These are the things we want to do." And we also want to hear from early career people as to what made them successful in addition to the people on the table. So to that extent, I look forward to INMM collecting, disseminating, and [making] assessments as to what's practical for us to pursue. And then to see if on the government side and working with international partners we can support some of these initiatives. But we will continue to emphasize our existing educational outreach programs. We'll look for every possible avenue to actually strengthen our commitment, if you would, in attracting and retaining people in our business.

Maria Betti: Thank you. Education and training is one of the key areas of interest for the European Commission and the JRC. Our Directorate General has introduced with the new structure — entered into force last July 1, 2016 — knowledge management units, one for each knowledge production directorate. These units are in charge of conducting the technical and scientific information scanning as well as managing dissemination and outreach activities, including trainings in collaboration with universities. As I mentioned this morning, we have several programs run together with our General Directorate of Research and Innovation promoting student exchanges in our facilities or in member state's facilities.

Also, the JRC organizes every year a decommissioning summer school. In Europe, there is an increasing demand of highly specialized workforce in the nuclear decommissioning sector. Providing young generation with hands-on trainings to obtain professional certificates is one of the key objectives of our summer school. We need to encourage students to engage in this specific sector, and not only in nuclear engineering or nuclear physics as done so far. We are also constituting knowledge centers with the objective to produce the scientific and political knowledge, combining it with generally acknowledged economics and the relevant social behaviors to disseminate highly meaningful and useful knowledge in specific areas of interest.

Glenn Abramczyk: This supports the material stored in Savannah River privately.

The one minute per ton. It appears five or six years ago we were going to have a nuclear renaissance and it didn't happen … So, it appears as if that's going to happen, it's going to happen with the new generation of nuclear reactors. How are your organizations working to incorporate safeguard security into those types of designs or facilities?

You are speaking about generation IV reactors, modern recent reactors. The JRC, however, doesn't conduct any engineering development activity in this field. Our involvement in the development of this kind of technology is first of all consultative: we participate in the generation IV discussions, speaking on behalf of the entire European Commission. We support our EU member states willing to develop these reactors in the frame of several consortia set up to this extent. For instance, one consortium is led by Belgians for the implementation of the MYRRAH project (Multipurpose hybrid Research Reactor for High-tech Applications). It consists of a subcritical, lead-bismuth cooled, fast neutron spectrum reactor coupled to a 600 MeV linear proton accelerator.

So far, we have been mostly involved in conducting safety study for these reactors. Very recently we have adopted a holistic approach to safeguard issues in collaboration with the IAEA that is also, very much involved in advancing nonproliferation. Very recently we have also included in the most recent programs a new type of modular reactor in the frame of a coordinated research project, in collaboration with the IAEA. We are currently focusing on the engineering part, the safety side, but also investigating the needs that the development of this kind of reactor may have in terms of workforce specialized in safeguards.

Brent Park: So it's interesting, as it turns out that the Fukushima event, there was a great hope and confidence that we were going to realize a renaissance almost overnight. And Fukushima happened. So there's a renewed emphasis on the safety in this aspect. These are the safeguards, meaning it has been progressing wonderfully. At the same time, what I just did with the IAEA a few weeks ago, we talked about microreactors. It's wonderful, the fact that the IAEA Director General is talking about small modular reactors and microreactors, and so I'm looking for peaceful end if they're used.

It's actually here appropriated. So what we are looking for as a committee is a life-cycle aspect of it from us. Not only designing it, building the reactors, but also the fuel side and actually using it safely and securely. And then what you do after it, right? You have to appreciate that tread life-cycle aspect of what it means to operate nuclear reactors, whether it's a regular or a small modulator or even microreactors and so on.

This is not a conversation the government could lead. This is not a conversation the users could lead. We have to work together by right. Again, there's a tendency to focus on what I call front of the design and building — not so much what you do afterwards. So that's where our organization was like INMM. They play a big role for people like me in government … . When people bring me half the solutions in the form of, "I want to design and build it," we have a problem. We need to actually to worry about what are you going to do with the spin fuels, for example. There's a life-cycle aspect that we need to talk about.

But again, we're hopeful that we have learned a lot from Fukushima and previous events. That we know how to make it safe, secure, and that we're all in operation that requirements and safeguards requirements and so on. [At the] system level, our challenge is not so much, "Can we design it?" Sure we can. "Can we build it?" Of course we can. But again, the guaranteeing safe and secure and safeguards, all those three words built in, it's hard. And the world is not that peaceful. I mean, there are always bad actors looking for ways to disturb our peaceful use. So to an extent, we have to do the best we can. But again, the life-cycle aspect of coming together, working with the community, government oversight, what they say in our CEO, part of my office looking to apply reasonable safeguards, control.

I strongly see a role of INMM in actually calling for a committee to get together. Let's have open discussion, and then I have to send my experts or even I participate in the conversation. But again, like you said about separate, there was conversation about separate silos and so on and so forth. We cannot go through that and at the end of that come up with a reasonable play. That's work ongoing. So it is quite important that we get together and talk about a system-level integration, life-cycle aspects of nuclear energy. And I'm in big support of small modular reactors and microreactors because it's less headache for us. Again, we need to look for unintended consequences along the way. And that's what we all do. Not just [inaudible 00:28:34] on the side, we being all of us around the table to an opportunity to discuss more.

Larry Satkowiak: Very good. Irmie?

Irmgard Niemeyer: Thank you. Well, I have a question for Dr. Park. Noting the impressive program and contributions on nuclear-related R&D, training and education in the U.S., including also international collaboration, I wonder how you see the role of the U.S. today, but also in [the] future, in promoting nuclear nonproliferation-related R&D, as well as training and education elsewhere, in particular in newcomer states and so-called developing countries. How do you see the role of the U.S. in supporting capacity building in nuclear nonproliferation in these countries?

Brent Park: Great question. In fact, that's a primary focus for one of the offices that I have within my own organization. We have a very strong outreach program. We actually take that challenge very seriously. Not everyone has resources like your country does or what our country does over here. Yeah, but to the extent that we can actually share our lessons learned, at the rate we send many of the instructors so they can train the instructors to make sure the training that we provide is focused at their level — at the users level in our partnering countries.

There's limitations, obviously. I mean,

the host countries or partnership countries, actually they need to step up. As for our systems, they definitely help, but also they need to step up their, what I call "donated level of participation." It cannot be just quote-unquote, we provide everything. There are limitations as to what we can do.

But again, in terms of — I am very much for international partners, whether they come over the U.S. or other developing countries, I really would like for them to get the best quality education. And in fact, if then when there is an opportunity for us to expand up a new education program, and I hope that there would be. To focus on safeguards and the NDC, all the things that we're talking about, that we hope to actually attract a fair number of international partners so that they could get advanced degrees. And then after they get trained, they go home. So that they would not only have relationships, but they would know the latest know-hows. So they can actually keep on working with us and at the same time, provide the best and the greatest service to their own countries.

This is an outreach program we take very seriously, to the extent that we set aside more than 20, 25 percent of my budget for international outreach program. We take it very seriously. We also work with, as you probably know, IAEA and other countries. We try to export our lessons learned. So when you have ideas as to how we can improve, I welcome those. And again, it's one of those that we want to work with the community and very close international partners. We would welcome input. So, whenever there's a way for us to upgrade, modify, enhance our international engagement, we'd be more than happy to do so.

Larry Satkowiak: Very good. Maria, do you have anything to add?

Maria Betti: No.

Larry Satkowiak: Okay. Jack?

Jack Jekowski: Thank you both for coming today and sharing some information with us. Bridging off of Felicia's question with the WINS challenge to provide certification for our membership, 18 years ago, the Institute really began to look at the issue of the "next generation of nuclear stewards" and where we were as an institution to ensure that the preparation of that generation was done adequately to fill our needs. Back in that timeframe, we didn't have any student chapters, so we started student chapters. J.D. Williams, who has since passed, and John Matter — who were the president and vice president at that time — had charged some members to develop the methodology for student chapters. And now we have 25 student chapters, both here in the U.S. and internationally. And we've struggled to help them as much as we can, both financially and in terms of support from the local chapters that are around them.

A couple of years ago, the Department of State, through the Partnership for Nuclear Security (PNS) picked up that baton, if you will, and made a special effort to engage with the development of international student chapters in a very spectacular way. They not only helped the establishment of those chapters, but they also paid for a substantial number of the members of those student chapters, and some international chapter members, to come here to the annual meeting. And they worked very closely with us and in partnership with them. That funding support has since largely gone away, but those chapters are still there and we now work very hard to support them.

So, as a piece to this process of making sure that we have a future generation that's well trained and certified, I hear you saying, "Come to us with your recommendations." And we'll certainly take that charge and do that. But do you have any perspectives on outreach, in particular to student chapters within the INMM, in terms of what might be done by your different organizations?

Maria Betti: Our outreach plans focus mainly on the European sector by first of all strengthening our relationships with academia, as a start. As, for instance, we are currently running doctoral partnerships with national-based universities. This initiative was launched last year; universities could apply for these grants in different fields, including nuclear. We tried to attract the best universities and those organizations/institutions with the most nuclear knowledge experience. These partnerships constitute the starting point for a more comprehensive program for collaborative partnerships on nuclear issues.

Talking about emerging topics of interest, we are currently working on nuclear nonpower energy applications. So, this means to exploit the nuclear knowledge for other applications such as nuclear medicine, support to the space policy by improving satellite systems, or application of nuclear in favor of environmental policies. Of course, nuclear engineering remains one important area of work, but we are also fostering research on other topics, mostly looking at the future evolution of the use of the nuclear knowledge, not necessarily limited to nuclear safety and security and safeguards.

Brent Park: So, that's a great question. As it turns out, one possible explanation, it has been known for decades, so it's something you know already. Every national lab to that extent, some of the sites and plants, it takes only a herd — literally hundreds of summer students, for example. I can easily foresee an organization, all these large national labs, quote-unquote, having a sister organization. Like the problem of "this society oversees," and so on and so forth. And it's something that our system could absorb without too much difficulty. But again, this requires that combination, a teaming, if you would, between the government sponsors and national lab sites and plants and universities and so on.

For example, as Los Alamos National Lab, that's where I actually did my PhD work in the '80s. And I was one of the literally five, six hundred students back there. And I was one of 400 PhD postdocs. And I can easily foresee that I had been playing a role in providing this — for the lack of a better word — introduction, if it's not been done already. But again, it doesn't take too much to actually make things happen. Oak Ridge, where I retired from a few months ago, has several hundred summer students from all over. But again, I think what we're talking about is a more focused engagement with the international student society that's been within this nuclear, quote-unquote, business. And it requires conversations with people like Larry Satkowiak and his cohorts and so on.

It's something that the people like me should be able to support easily. What I call a no-brainer. But again, you need to initiate that. And your example of a state park on helping out. Chances are, what the government can do is a 1-year, 2-year thing. You need to seize the moment then and make it more sustainable again, that this is a chance for the entire membership. The way I see it — because I come from the lab background, almost 30 years — you will not break a bank to make this happen. I talked about our three sectors of excellence. One led by Berkeley, one Michigan, and one North Carolina. We're doing it already within the U.S. system. One thing that I actually did mention is that all these university consortia, lab partners. And anyway, there are enough great examples that you can actually learn from them. And I am certain that you can easily find a great solution within the system that we already had.

It's actually relatively easy to absorb a clinical year if we want.

Larry Satkowiak: Chris.

Chris Pickett: Okay. Both of you mentioned the need to preserve knowledge and critical skills in this profession. I'm an advocate of using R&D to do some of that, especially when the R&D program is set up to fund, mentor, and protégé. Looking out over the next decade, what do you see are the nonproliferation and safeguards R&D challenges that current- and next-generation researchers should be trying to address? We won't limit you to your budgets.

Brent Park: Well, probably. So, let's see, 30 years ago … No actually, I found out much later that many of the mentors that I had were quote-unquote godfathers of the weapons programs. I didn't know they wrote the textbooks that I studied with. And they thankfully took time to educate me, train me. And I learned from the best, by the best, so we need to ask ourselves, are we spending that kind of quality time with the next generation? And it's easy to ask around, are you doing it? But are you doing it yourself is the question, right? And that's something that you cannot ask others, but you have to look in the mirror. I use this phrase all the time with my staff. You have to look in the mirror and say, are you doing it? That's how you start.

And it's not a grand, big plan that will fix the truck or arrest the challenges. I think it's more of an individual level, the participation and your commitment. So to a big extent, I just don't believe having a big slogan and putting it up … Well, it might help, it would not hurt. But it's not a money ship, by the way. Money will not solve that challenge. The people well before me, most of them passed away. But again, they actually took time out of their busy schedule to teach me, train me. And I will be doing something in return. I am, but not as much. I'm not sure why, but I'm weaseling out of that. Answering that question so you may end up on it.

But it's an individual thing, really. It's not because on the weapons program side, we put tens of millions of dollars to preserve knowledge and all of that. Guess what? It's all at the individual level. And I strongly believe we have to do it, you have to do it, I have to do it. And okay there's big program money behind it. You just have to take time. I'm sure my PA guy is stressing out right now.

Maria Betti: I could first try to address your question by referring to the challenges ahead of us and particularly marking the next decade with reference to nonproliferation issues. This is a very interesting subject as it allows us to brainstorm and possibly make some reliable predictions on the future. Personally, I see the challenges linked to proliferation related strictly to the evolution of IT systems. I don't believe we will face increasing smuggling of nuclear material. I believe that smuggling of data or engineering applications will be more likely in the future than smuggling of physical things. If we look at the IT evolution, cybersecurity and nuclear cybersecurity are amongst the main issues at stake at present. This type of smuggling could enter directly in the nuclear cycle, in the nuclear plants or reactors, in nuclear weapons development. This is my personal view only.

Larry Satkowiak: Very good. Rian.

Rian Bahran: So I think that the

national labs at the universities and the NGOs have done a great job with outreach and trying to talk to academics about students verification. And so, I think there's a lot of good institutional programs, including the university consortia and others out of your office. So we are getting a lot of students at the national laboratories. There are some great mentors from Haas Laboratory, some that I'm seeing here, previous departmenters. But the problem that we have is retaining the next generation. So, we do a good job to bring students in, but how do you keep someone at the national laboratory if they have offers at Google? This is a question that people discuss and the notional answer is, "Well, you tell them, if you go to Silicon Valley, you can pretend to save the world. And if you go to New York City and go to a hedge fund, you just say, 'I don't care about saving the world' and make a ton of money. But if you work at the national lab, you actually get to save the world."

And that works sometimes, but I think we need to do better at telling stories. It goes back to scientists can't talk to politicians because scientists aren't good at telling stories. And it's the same thing with retention. How do we tell more specific stories? How do we tell better stories? There's a lot of things that your organization, you guys are involved in, things that maybe you talk to policymakers about. So those are the same messaging, some of the same things that we can use with students to really get them to buy into the value of this profession. So, with that said, I think that we can do better on messaging, and I think we can learn from what your organizations do at a higher level and distill that down. Do you have any thoughts on that?

Maria Betti: So far my remarks have mostly focused on nuclear knowledge. However, 60 years ago when the Euratom Treaty was signed, nuclear was considered as a revolutionary source of sustainable energy production. The past 60 years of nuclear exploitation in the energy sector have confirmed these expectations, and that's exactly what nuclear has provided us with. The problem that we encountered and couldn't solve was how to treat the nuclear waste, which remains the main issue nowadays deriving from the use of nuclear for energy production. My dream would be to finally find a permanent and sustainable solution to the treatment of nuclear waste in the frame of the circular economy approach.

Now, today nuclear is still considered as a major threat and is still scaring many. We must find a way to invert this perception and do our best to convey a positive message about nuclear knowledge. Now if you go into the hospital and need to do a tomography, you have to use nuclear technology. If you want to do a positron emission analysis, you have to use nuclear technology. If you do radiotherapy for treating cancer, we need the nuclear technology. If you use the radio isotope to treat the cancer or leukemia, you need to produce a radio isotope. Each and every citizen is accepting nuclear for these scopes.

Of course, in order to produce radioisotopes for nuclear medicine, a reactor is needed, and it must be run by securing its safety and by granting also security and safeguards standards. This is how we might start a counter-narrative: by putting the focus on the positive use of the nuclear as knowledge as well as on all the different possible applications of this use, because we need to maintain this knowledge. This is the future. It is clear that we cannot simply accept to dismiss nuclear for producing energy. Nuclear must keep on accounting in the global energy mix for the 20% at least until we don't reach the famous 2-degree objective [2 degrees Celsius of the warming limit]. Each member state in Europe asked to choose its own energy mix; therefore, we cannot impose nuclear, but it is sure that this energy source will remain for decades.

We have to start talking differently to people. Nuclear is knowledge, is a science. And we cannot be afraid of nuclear because if we would have been afraid of the fire when the man of the stones found it, today we wouldn't have electricity, we wouldn't have achieved progress and modernization. So we should not be afraid of things. We should explore it for positive purposes, for the good of all.

Brent Park: You did not let me off. It is a big challenge. So, myself, [it's] quite different, given it was 10, 20, 30, 40 years ago. So I have a grown daughter working in the Bay Area, and I have great expectations for her. That's how many of these next-generation people see their career path — not staying with one company. That's the reality. We need to appreciate it. But the flip side of it is, I was actually thinking about retention and numbers that my people provided yesterday, this morning. This fellows program. I actually mentioned that we actually have graduated about 453 people. This year we got 53 fellows. Retention is high 90s. So what's the difference between the general public next generation and the fellows that we have? The fellows that I have are actually much more seasoned, by the way, than our first grads. Many of them do have masters and some have PhDs, and they're not really young-young, out of college, for example.

And when I think about them, in fact, I have a few in my front office. In fact, they stick that span about a year and they get to decide whether to stay or not. These people are connecting to doing something meaningful and they are appreciated for what they do. And I think that's a key to retain people. That they're appreciated. And they work long hours, by the way. It's basically at my front office, so they show up and many of them work after I'm gone.

But again, it's a meaningful assignment and that's not easy. As it might sound, by the way. Because especially now, business, for those of us who are in the national security business, you have to get clearance and you have to wait so many years and so on and so forth. And it's hard to give that meaningful assignment. But again, when I look at the fellows program, where it's open to the general public, that's a big difference. Again, I attribute it to meaningful challenging assignment. They don't mind long hours, by the way. They love to work as long as it takes to get the job done.

And I think it is, the intention is more of, "Are they happy doing what they're doing rather than whether they're making an extra buck or not?" And once a year they worry about their salary, whether I get my 10% raise or 1% raise, that conversation is over in two hours. And whether they like working with, working for a supervisor is a big challenge. Whether they have a meaningful assignment is not about a glamorous project. It's something that they can put their hands on. And that's actually our collective challenge, we talked about retention all the time as it is a foreign concept. It's not. It's what you want to get out of your supervisor and your working environment, too. You want to be appreciated, you never complain [about] long hours when it's meaningful. And when the product has to be delivered, you work extra hours, who cares?

And again, I think it is, even if it is mundane, we need to find a way for them to remain corrected in couple, then. Engaged for the project. Rather than just giving the peripherals, information, background, and what not. They're not depreciated, right? They know they're not appreciated, they leave. Okay. And I'm not sure if I'm answering your question, but retention could be … handled in many different ways. What's your way? Again, looking at my fellows program. Retention rate, you cannot have 98 percent retention. They work the long hours, by the way. Headquarters is not the easy place to work out of, by the way. So, I could go on and on and on. But again, meaningful challenge and assignment. And the young people with their creativity, you need to listen to them.

But it is more of a "how" than a "what" when it comes to retention. So yeah, it's a tall challenge for all of us.

Larry Satkowiak: Thank you. I was going to have Corey ask her question, and then I'm going to cut off the questions and allow our speakers to make concluding remarks if they so desire.

Corey Hinderstein: My question was coming back to the issue of international safeguards and verification. And kind of how ambitious should we all be? Safeguards is one example, but maybe it's not the only one. When we look at the Additional Protocol, which I know both of your organizations support both from a policy level as well as at the technical level, it's the gold standard right now, but it's also 21 years old. In no other part of our assessment of nuclear threat and nuclear risk do we look at the solutions we came up with 21 years ago and say, "That's good enough."

Should we be thinking about what comes next? And how do we build on or expand on the principles that were addressed through the Additional Protocol. Or, is the AP good enough, and our job should be to make sure it's implemented to the greatest extent possible?

Brent Park: So, every four years you can get the new and improved version of whatever initiative you have, right? And that's how we sell things. In fact, this isn't that different, as it turns out. Going back further, international engagement, verification and so on and so forth. The key word that comes to my mind is transparency. That's how we actually know that it's a peaceful co-existence if I can use that phrase over and over again, that we're heading for. Not one nation imposing its own policies and whatever, right? After all, what are we trying to achieve out of advanced protocols and so on. That's so that the peaceful civilian energy program is kept as such.

And today's understanding of the frame is correct, is we will continue to write it. But in terms of how we implement it, there is a constant, ongoing, continuous development that we need to actually pursue. And so what may take a month for us to find out should take only maybe half a day. So it's a different kind of an R&D. What works on the bedside is not what we're looking for. And this morning, I briefly talked about the fact that the AP is more like all of it. I think, that if it works on my bench, so I'm not sure why it's not working out in the field, then that instrument doesn't really serve any purpose. But at the same time, we need to push the envelope on the R&D side so that we actually have hope to deploy the latest and the greatest. There is a gap somewhere that we need to address.

But when it comes to effective engagement, AP and whether we have room to improve, the answer is absolutely yes. There is room to improve. But again, much of that, as you know, Corey, international engagement is people to people.

Sometimes that is in the way rather than technology. So the transparent, open communication as to what we are looking for. Again, it's a peaceful co-existence that we're looking for, we're looking to sustain. And to that extent, we have a lot of homework to do, especially people on my side. But again, like I said on previous topics, I look for ways to enhance. It's not all technology-driven exercise. It's people getting to know each other and know how each other's — we don't all speak the same language. God knows I speak a half language, the other half is all numbers and equations, right? As a dumb physicist. So it's important that we build a relationship, so oh yeah, INMM has a great role to play. We actually invite the international partners to this international program that we have. So to the greatest extent, I really applaud INMM doing its job as a broker, as a go-between, peacemaker, call it whatever you need to.

But again, it has a very important role to play so that we can actually exchange ideas and thoughts and try to enhance ... I keep on using this same phrase, a "peaceful co-existence." A peaceful use of the nuclear energy, and so on.

Maria Betti: Thank you. The Additional Protocol has been one milestone achieved in the frame of advancing safeguards, very much related with technology for environmental monitoring. And it's really a protocol that allows transparency between those countries that decided to sign and adopt it. As I have done this morning during my intervention, I encourage and hope that those countries that have not yet signed it will sign in the future. Trust constitutes a very solid background to start communicating more openly.

From a technological point of view, I don't know if more could be done to realize an Additional Protocol. What could be added to the Additional Protocol is the trade control. This could be the next step, going in the same direction, carrying on the same philosophy of the Additional Protocol.

Larry Satkowiak: Very good. So, I'm going to allow our two speakers some concluding remarks if they so desire. They can pass.

Maria Betti: I have one main concluding remark: I believe that the community of professionals — and by "professional," I mean all categories of those working in this field — should stay together, communicate, exchange ideas, debate, in order to find solutions that are possible, doable, and acceptable for the countries tackling their responsibility in granting security for the sake of people. So they have to accept to evaluate proposals, be transparent and trustful. These are my conclusion on the issues.

Brent Park: So, thank you. I don't know what I got myself into when I said yes to Teressa and agreed to come over and say hello to you. But the INMM is an impressive organization. And looking around the table, we have a very knowledgeable and responsible people in the leadership positions. So I appreciate that. In fact, there is not yet another organization like INMM serving the purpose that you serve. And thank you for all that you have been doing for 59 years. It's a big deal. It's older than me by a few years, which is shocking. I wish you all the best in our years and hope to engage more effectively with you. And don't be shy, not that you guys are ever shy, about letting us know what your thoughts are and how we should reach out. You don't let other people do that, why don't you? So please let us know.

And we also have a fairly effective membership and leadership team. Obviously there's Corey and Larry and Teressa and everybody else. And good luck to you. I don't know how they're going to capture this body language on the transcript. But again, with the people like Holgate and many others in the membership, I think that your interest, which is my interest as well, are really nicely covered. I applaud you for focusing on the students, next generations. And I truly appreciate working with the international partners.

Actually, that's what my office is all about at the end. My corporation is all about international partnership and the peaceful use of nuclear energy. But, to that extent, again, I thank INMM for inviting me. You guys are awesome. And again, I appreciate it. Thank you so much and good luck to you. I wish I could help out along the way. And I think I've got some good ideas from talking with people today. So again, thank you, great job, keep doing it.

Larry Satkowiak: So I want to thank everybody that participated in the luncheon. And in particular, I want to thank our two plenary speakers. They were terrific, not only this morning, but also putting up with us during lunch and answering our questions. Thank you again.

Game-Theoretic Allocation of Security Investments at Nuclear Reactors

By David Morton

Abstract

This paper presents a game-theoretic model to guide defensive strategies for securing a nuclear facility against an attack by a highly rational and knowledgeable adversary. In our sequential play formulation, the defender chooses and implements security upgrades from a given portfolio subject to a budget constraint and in expectation of a fully informed and rational adversary. Then the adversary observes which upgrades are implemented and chooses an attack that maximizes the expected consequence. Hence, we model the situation as a two-person zero-sum game with fully symmetric information. We represent the facility as a directed graph of nodes and arcs, within which adversary capabilities are reflected via nondetection probabilities and travel times across each arc. By correlating the security force response time and probability it will defeat the adversary with the arc where the adversary is detected, we correlate the force-on-force defeat probability with the time the defender has available to prepare for the engagement. We analyze results of the model when defending against an adversary who is targeting the heat sink or offsite power supply components of a reactor. Finally, we evaluate the impact of changes in cost or effectiveness of different solutions on both the defender's optimal set of solutions and the adversary's chosen path.

Keywords: Game theory, Stackelberg game, security model, physical protection system, nuclear power

Introduction

Overview

We present an innovative security investment decision-making approach for physical protection systems at nuclear facilities. Our approach applies a game-theoretic model to a set of security investments to most effectively defend against an intelligent adversary with full knowledge of the facility and its defenses. The game-theoretic framework is informed by a pathway model of the physical protection system (PPS) of a nuclear facility. The pathway model determines the probability an attacker is defeated given an adversary–defender strategy pair. An adversary strategy is defined by the pathway taken through the facility to reach the selected target and exit. Each defender strategy is composed of a portfolio of PPS investments.

The objective of the adversary is to maximize the damaging consequences of his attack. Damage to a nuclear facility could involve theft of nuclear material, release of radiation to the environment, or structural damage to the nuclear island or other elements of the facility, to name a few examples. The demonstration case we present considers a generic nuclear power plant layout with just two potential targets, both located outside the nuclear island: the ultimate heat sink and the electrical switchyard. A successful attack gives rise to monetary and nonmonetizable consequences; our method assumes that each target can be assigned a relative consequence value. To the adversary, the game-theoretic payoff is the consequence of his attack multiplied by his likelihood of successfully carrying out the attack, with the defender's payoff being equal and opposite. We term this payoff the *expected consequence*.

We model the defense of a nuclear facility against an intelligent adversary, starting from an analysis of pathways through the facility with baseline physical protection measures in place. We then use our game-theoretic model to determine the pathway that an intelligent adversary with complete information about the facility would traverse by stealth or force in order to sabotage a target, given that the defender has applied security upgrades to the system. While we do not use authentic security data in the model, we aim to demonstrate the ability of this model to compare the costs of the resources required to pursue various options for hardening the facility with benefits of improved facility security.

Our adversary attempts to inflict the maximum expected consequence while still managing to escape the facility. He chooses between multiple targets with unique defenses and payoffs. The defender aims to detect the presence of the adversary inside of the facility in time to send a response force to neutralize the adversary before he escapes. Given the defender's strategy, one adversary strategy is to sneak through the facility undetected until he can outrun the response force and still achieve his goal, at which time he races through the facility without concern for being detected. The model also incorporates a probability of the adversary defeating the response force. A crucial strength of the game-theoretic approach is that we do not specify the adversary's strategy; instead, given complete information, the adversary chooses his attack strategy from among tens of thousands of available options.

Our model has the defender select security upgrades subject to a budget constraint. The defender has a range of investment options, each of which has a cost and benefits, such as increasing the probability of detecting the adversary, slowing the adversary's travel, or enabling a faster or stronger response force. Since the defender guards against an adversary who is endowed with complete information concerning the facility and its defenses, the defender makes upgrade decisions with the knowledge that the adversary will be aware of them in choosing a route through the facility. As a result, the defender's investments typically change the adversary's preferred route and target. The defender chooses upgrades with the objective of making the adversary's most attractive pathway to each target as undesirable as possible, consistent with the expected consequence's measure of desirability.

These results allow us to conduct a cost-benefit analysis for investment options. Central to our analysis is a narrative of the security upgrades the defender chooses to implement at each budget level and their effects on adversary behavior. We use this analysis to depict the best possible return on investment at each budget level — that is, the efficient frontier.

Literature Review

The literature includes a number of applications of game-theoretic models to system security. There are various names variants of these models, including interdiction models, bilevel attacker–defender models, trilevel attacker–defender–attacker models, and security games, which tend to be a mix of Stackelberg and/or Cournot games. Some studies focus on selecting inspection strategies for detecting smuggled nuclear material. Gaukler et al.[1] and Wein et al.[2] use queueing models at a seaport and study the defender's multilayered security system in which the defender seeks to optimize the inspection strategy while constrained by increases in congestion. Additional studies focusing on nuclear material interdiction include Boros et al.,[3] Madigan et al.,[4] McLay et al.,[5] and Stroud et al.[6] Dimitrov et al.[7] and Nehme[8] each describe models that investigate how to secure a large-scale transportation network against a smuggler of illicit nuclear material. The work of Dimitrov et al.[7] and related work of Morton et al.[9] and Pan et al. [10,11] have connections to our model in that they feature an adversary attempting to traverse a network without being detected, as well as a defender seeking to maximize his detection probability by installing assets on the network. Atkinson et al.[12] describe a model that locates detectors in and around a city, where the adversary seeks to reach as close to a city-center target as possible before detonating his nuclear device.

Game-theoretic models differ from probabilistic risk assessment (PRA) approaches to security. PRA has its origins in assessing the likelihood of natural or nondeliberate hazards, where probabilities of particular types of failures must be assessed. Under the PRA approach to security, one assigns probabilities to the likelihood that an adversary will attack in a particular manner.[13] In contrast, in a game-theoretic model, these probabilities are an output of the model rather than an exogenously specified input. In this way, the probability that the attacker selects a strategy in a game theory model is not static; rather, it adapts to the manner in which the defender hardens his system. The National Research Council has criticized the use of PRA in modeling terrorist threats due to this limitation of PRA.[14,15] For more perspective on PRA in comparison to game-theoretic approaches, see the work by Brown,[16] Cox,[17,18] and Golany et al.[19]

The literature has a limited number of applications of game-theoretic models directly related to nuclear facility security and counter-proliferation. Ward and Schneider[20] implement a model to design safeguards against insider misuse or diversion of materials from a nuclear fuel cycle facility under International Atomic Energy Agency (IAEA) safeguards. Brown et al.[21] describe a model to delay an adversary's development of a first nuclear weapon. The underlying system operation model in this case is a PERT-CPM network for the adversary's project.[22]

There are important applications of game-theoretic models to security for non-nuclear facilities and systems involve hardening critical infrastructure to attack. In these models, the underlying operations model involves the system of critical infrastructure. Salmeron et al.[23,24] studied vulnerabilities in an electric power system by building a model to optimally attack that system. A series of papers describes how to locate detectors in a municipal water system to rapidly detect contaminants injected in that system.[25–28] Further security challenges to which game-theoretic models have been applied include communications systems,[29] airport security,[30] municipal transportation networks,[31] and the U.S. Strategic Petroleum Reserve.[32] See Alderson et al.,[31] Brown et al.,[32] and Dimitrov and Morton[33] for overviews and further discussion of these types of models.

The adversary's ability to use stealth and then speed to traverse a network of pathways, as well as the distinction between the detection and defeat of an adversary, is featured in other PPS analysis techniques,[34] although not in the context of the type of optimization models we employ.

The remainder of this paper is structured as follows. Section 2 formulates our model and introduces a problem instance, while Section 3 gives a summary of results from this instance. Finally, Section 4 discusses the information that can be gleaned from the game-theoretic approach, as well as possible ways to extend these models.

Model Description

Network Structure and Safeguards

In this section, we describe a network that allows an adversary to choose between two targets at a nuclear facility: the cooling towers and the switchyard, as shown in Figure 1. The cooling towers consist of a standard open circuit (wet) tower design, counter-flow or crossflow, with all components (cells, condenser water pumps, etc.) located within the limited area of the facility. All primary tower components are located together, so there is effectively one single "tower" target. In addition, there is one switchyard located within the limited area, which represents another single effective target. The PPS for these targets is based on guidelines laid out by the IAEA and the U.S. Nuclear Regulatory Commission. They advocate for security that is graded according to the locations of desirable targets and which maintains defense-in-depth strategies; this leads to a layered structure of defensive areas that increase in security strength as one travels deeper into the facility.

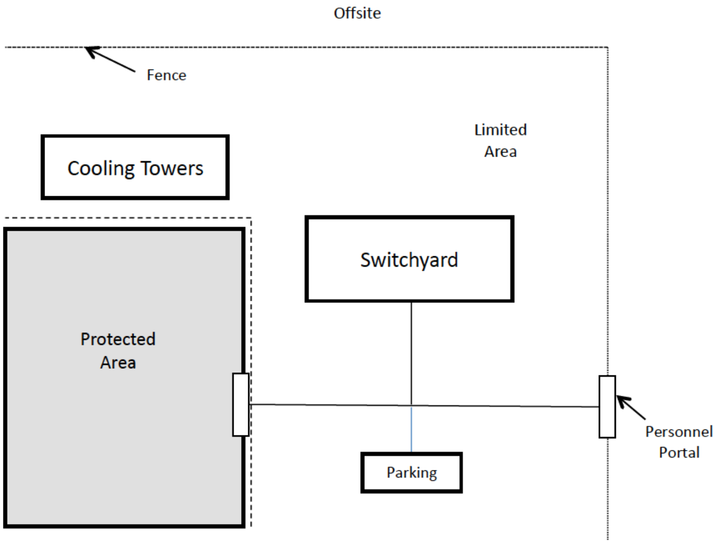


Figure 1. Conceptual depiction of the facility

We model the facility as a directed network of arcs and nodes, as shown in Figures 2 and 3, with nodes representing locations and arcs representing paths between two locations (nodes). The lack of an arc between two nodes reflects that it is impossible for the adversary to traverse directly from one node to the other, or that there is no rational reason for the adversary to pursue such a path. We assign a nondetection probability and a travel time to each arc. These quantities reflect our characterization of the adversary's capabilities.

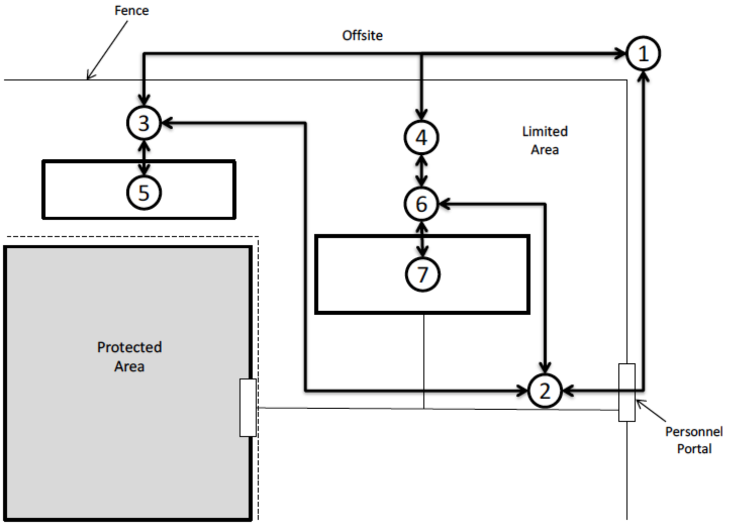


Figure 2. Network overlay of the facility

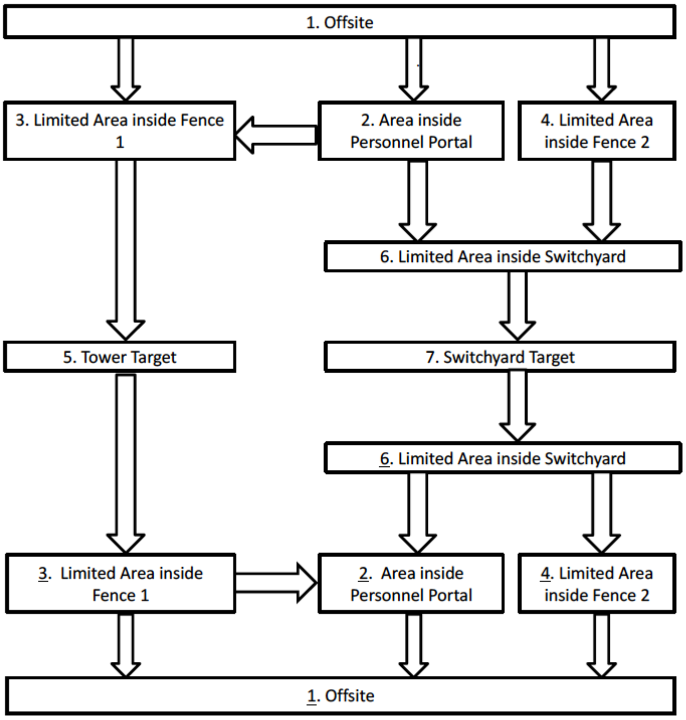

1. Offsite
3. Limited Area inside Fence 1
2. Area inside Personnel Portal
4. Limited Area inside Fence 2
6. Limited Area inside Switchyard
5. Tower Target
7. Switchyard Target
6. Limited Area inside Switchyard
3. Limited Area inside Fence 1
2. Area inside Personnel Portal
4. Limited Area inside Fence 2
1. Offsite

Figure 3. Mirrored network representation of the facility[36]

Because the adversary succeeds only by both attacking the target and escaping the facility, we depict the adversary's path using a mirrored network in which the first half of the network contains pathways to the target and the second half (the reflection) contains paths of egress. Travel times and nondetection probabilities can differ on these two halves of the network, and the ingress and egress networks themselves need not be perfectly symmetric. Note that nodes in Figure 3 with an underscore indicate that the adversary is leaving the network through the node after attacking a target, rather than approaching a target.

We populate the arc nondetection probabilities and travel times by assessing the set of obstacles that can either detect or delay an adversary traversing the arc and then estimating the probability of detection and time delay associated with each obstacle. The nondetection probability is the product of the nondetection probabilities of each obstacle, and the travel time of the arc is the sum of travel times of each obstacle plus the time to travel the distance between locations. A previous publication[35] presents this methodology in greater detail. The data in this model was constructed for use in student exercises for vulnerability analyst training, and it is not appropriate for use in actual security analyses. Using these sample values, which were also presented in our previous work,[35] we populate the network seen in Figure 3. The resulting travel times and nondetection probabilities are shown in Table 1 on the following page.

To incorporate the paradigm of an adversary using both speed and stealth into our game-theoretic approach, we depict a facility by two parallel networks having common nodes and arcs. One network describes an adversary sneaking through the facility and is characterized by evasion probabilities, given that the adversary is using stealth without regard to travel time. The other network, to which the adversary may choose to switch at any point within the facility, gives travel times which depict the adversary moving at the best speed without regard to detection to reach his target and flee the facility ahead of the response force.

Assumptions

Our model has the following structure and assumptions.

1. Our adversary has complete information regarding the facility. That is, the adversary knows the layout of the facility, the nondetection probabilities and travel times for all arcs, his chance of overcoming the response force, and the response time of the security force. Also, the adversary and the defender both know how each security upgrade would affect the nondetection probabilities and travel times of the arcs. Finally, the adversary assigns a consequence value to each target he may attack within the facility.
2. The defender and adversary agree on every item listed in assumption 1 and place the same value on the consequence of damage to each target.
3. The defender optimally chooses a subset of security upgrades to implement according to a two-person Stackelberg game. Upon observing implemented security upgrades, the adversary then attacks the facility so as to maximize the expected consequence.
4. The two-person Stackelberg game is zero-sum. That is, the adversary's objective (to maximize the expected consequence) is diametrically opposed to the defender's objective (to minimize the expected consequence). This assumption reflects our view that we should model the *capabilities* of the adversary rather than attempting to model our belief about his *intentions*.
5. The adversary has a nonunitary defeat probability should he encounter the security response force. That is, if a force-on-force scenario ensues, the adversary has a known chance of defeating the response force. This

Table 1. Number and location of obstacles in baseline facility

Path	Path Type	Fence	Personnel Portal	Stationed Guards	Random Searches	Nonguard Personnel	Roaming Guards	Alarmed Detection Device	Video Surveillance
1 → 2	Personnel		1	1	1				1
2 → 1	Personnel								1
1 ↔ 3	Fence	1				1	1	1	1
1 ↔ 4	Fence	1				1	1	1	1
2 ↔ 3	Property								1
2 ↔ 6	Property								1
3 ↔ 5	Attack Tower	1				1	1	1	1
4 ↔ 6	Property								1
6 ↔ 7	Attack Switchyard					2			1

Path	Nondetection Probability	Travel Time (sec.)
1 → 2	0.86	35
2 → 1	0.97	10
1 ↔ 3	0.73	50
1 ↔ 4	0.73	50
2 ↔ 3	0.91	60
2 ↔ 6	0.91	60
3 ↔ 5	0.72	120
4 ↔ 6	0.91	60
6 ↔ 7	0.85	50

probability is a function of where he is detected within the mirrored network. As we discuss in Section 3, if the adversary is detected sufficiently early in his attack to allow the response force time to fortify an advantageous position, the security force's probability of defeating the adversary increases.

6. If the adversary reaches the *critical detection region* without having been detected, then he succeeds, because he is able to escape before the response force arrives. The critical detection region is the set of all nodes (locations) from which it is possible for the adversary to escape the facility before the response force can reach him. We refer to nodes in the critical detection region as escape nodes.

7. The adversary can also succeed even if he does not reach the critical detection region without having been

8. detected. This requires that the adversary defeat the response force, which we assume occurs with known probability. A simple variant of the model would allow the adversary to succeed merely upon reaching his target.

Mixed-Integer Programming Formulation

The two-person Stackelberg game is formulated by use of a mixed-integer program (MIP). We introduce the formulation with a minimax objective function, as the adversary will choose the path of highest expected consequence for any set of security upgrades implemented by the defender, and the defender seeks to minimize the expected consequence of the best path for the adversary. In order to succeed, the adversary must traverse the network, reach one of two targets, and either (1) travel undetected to a node from which he can escape or (2) defeat the response force.

Indices and sets

$i, j, k \in N$ nodes in the network representing locations in the facility

$(i, j) \in A$ arcs in the network representing allowable movement from *i* to *j*

$i, j, k \in N_t$ all nodes in the network associated with targeting the towers

$i, j, k \in N_{sw}$ all nodes in the network associated with targeting the switchyard

$s \in S$ security upgrades

S_{ij} subset of security upgrades that can be applied to arc *(i,j)*

1 and n *1* is the offsite origin node and *n* is the offsite terminal node in the mirrored network

Data

p_{ij} adversary's nondetection probability when traversing arc *(i, j)*

p_{ijs} adversary's nondetection probability when traversing arc *(i, j)*, given security upgrade *s*

t_{ij} time required for adversary to traverse arc *(i, j)*

t_{ijs} additional time required for adversary to traverse arc *(i, j)*, given implementation of security upgrade *s*

c_s cost of security upgrade *s*

R_{ij} response time of the security force if the adversary is detected on arc

α_{ij} adversary's chance of overcoming the response force, if detected on arc

M large number; suffices

B defender's budget

D_t defender's valuation of damage for a successful attack to the towers

D_{sw} defender's valuation of damage for a successful attack to the switchyard

Defender's decision variables

x_s binary variable indicating whether the defender implements (*xs = 1*) security upgrade *s* or not (*xs = 0*)

w the expected damage that the defender incurs

Adversary's decision variables

π_{ij} adversary's probability of successfully reaching node *j*, given that he is currently at node *i* and undetected, assuming that he moves from *i* to *j* so as to maximize this probability

τ_i time to reach node *n* (facility exit) starting at node *i*, assuming the adversary follows the shortest-time path from *i* to *n*

s_i binary variable that indicates whether or not node *i* is an escape node; i.e., a node in the critical detection region

Boundary conditions

$\tau_n \equiv 0$ time to reach terminal node *n*, given that the adversary is at node *n,* is zero

$s_n \equiv 1$ the terminal node is an escape node, and hence this binary is one

$\pi_{jj} \equiv 1$ probability of successfully reaching node *j*, given that adversary is at node *j*, is one

Model formulation

$$\min_{\tau,w,s,x,\pi}\ w \tag{1a}$$

$$\text{s.t.}\quad \pi_{ij} \geq\ \alpha_{ik}(1 - p_{iks}) + p_{iks}\pi_{kj} + \textstyle\sum_{s\in S_{ik}} x_s - 1, \forall\ i, j, k\ \in N, (i, k) \in A \tag{1b}$$

$$\pi_{ij} \geq\ \alpha_{ik}(1 - p_{ik}) + p_{ik}\pi_{kj} - \textstyle\sum_{s\in S_{ik}} x_s\,, \forall\ i, j, k\ \in N, (i, k) \in A \tag{1c}$$

$$\pi_{ij} \geq\ \alpha_{ik}\ \forall\ i, j\ \in N, (i, k) \in A, p_{ik}\ \neq 0 \tag{1d}$$

$$\tau_i\ \leq\ \tau_j +\ t_{ij} + \textstyle\sum_{s\in S_{ij}} t_{ijs}x_s\,, \forall\ (i, j) \in A \tag{1e}$$

$$\tau_j + t_{ij} + \textstyle\sum_{s\in S_{ij}} t_{ijs}x_s - R_{ij} + Ms_i\ \geq\ 0, \forall\ (i, j)\ \in A \tag{1f}$$

$$w\ \geq\ \pi_{1j}D_t -\ (1 - s_j)M, \forall\ j \in N_t \tag{1g}$$

$$w\ \geq\ \pi_{1j}D_{sw} -\ (1 - s_j)M, \forall\ j \in N_{sw} \tag{1h}$$

$$\textstyle\sum_{s\in S} c_s x_s \leq B \tag{1i}$$

$$\textstyle\sum_{s\in S_{ij}} x_s \leq 1, \forall\ (i, j) \in A \tag{1j}$$

$$\pi_{ij}\ \geq 0, \forall\ i, j \in N \tag{1k}$$

$$\tau_i\ \geq 0, \forall\ i \in N \tag{1l}$$

$$s_i\ \in \{0,1\}, \forall\ i \in N \tag{1m}$$

$$x_s\ \in \{0,1\}, \forall\ s \in S \tag{1n}$$

The objective function in (1a) reflects the goal of the defender to minimize the expected consequence incurred from an attack by the adversary. Constraints (1b) through (1d) capture the assumption that if the adversary is at node *i* and undetected, then he will move to node *j* so as to maximize his probability of successfully getting there. Here, success takes into account nondetection probabilities, but also , the adversary's chance of overcoming the response force if detected on that arc. In one extreme case, a maximum-reliability path (stealth) may be optimal. At the opposite extreme, if the values of α and/or *R* are sufficiently large on an adjacent arc, then the adversary may find it optimal to "intentionally" be detected — constraint (1d) — and attempt to overcome the response force (forceful adversary). Again, if the adversary overcomes the response force, then we assume he achieves his objective with certainty.

If a security upgrade is implemented on arc *(i,k)*, then constraint (1b) applies, whereas (1c) is vacuous. If no security upgrade is implemented on arc *(i,k)*, then constraint (1c) applies, whereas constraint (1b) is vacuous. Note that as captured by constraint (1j), we assume only one security upgrade may be applied to a given arc.

Constraint (1e) reflects the adversary's choice of a *shortest* path through the facility. Here, the notion of shortest path implies the path of least travel time from node *i* to the facility exit, and so it represents the adversary's quickest escape route from his current location. The adversary follows this route upon reaching the critical detection region. Constraint (1e) also accounts for the fact that travel time across arc *(i,j)* is lengthened if the defender implements an applicable upgrade.

Using the known response times of the security force (*Rij*), constraint (1f) determines whether node *i* is in the critical detection region. If any node adjacent to *i* — say, *j* — is such that $\tau_j + t_{ij} < R_{ij}$, then *i* is an escape node. Constraints (1g) and (1h) capture the fact that the adversary selects a path to maximize expected consequence. The expected consequence is the largest product, across all nodes in the critical detection region, of the adversary's probability of reaching that node, and the target value associated with the path he took to reach that node.

Constraint (1i) is a budget constraint limiting the number of security upgrades that the defender may implement. Constraints (1k) and (1l) are non-negativity bounds. Finally, constraints (1m) and (1n) enforce binary restrictions.

Baseline Problem

Based on the multitarget mirrored network and the MIP formulation, we begin this section by defining the following *baseline* problem, which has a zero budget (*B* = 0) for security upgrades. The baseline network has in place the default security measures of Table 1. Hence, even in the absence of the upgrades we present below, an adversary is confronted with significant security measures. Numerical parameters listed in this section are again for illustrative purposes.

- *Critical Detection Region 1 (CDR 1)* – This region includes all nodes from which the adversary can escape the facility more quickly than the minimum response time of the security force (70 sec.). If the adversary reaches a node inside CDR 1, then the adversary successfully completes his attack.
- *Critical Detection Region 2 (CDR 2)* – This region includes nodes from which the adversary cannot escape prior to the minimum response time of the security force (70 sec.) but is within a longer time interval (100 sec.) of escaping. While the response force can reach the adversary if he is detected within this region, the force will have limited preparation time and suffer a reduced chance of defeating the adversary. If the adversary is detected at a node from which he requires more than 100 seconds to set up his attack and escape the facility, then the response force has more time to choose and fortify the site of battle.
- *Response Force Strength* – If the adversary is detected prior to CDR 2, thereby allowing the defender more time to prepare for the battle, then the response force has a probability of 0.9 of defeating the adversary and thus foiling the attack. If the adversary is detected within CDR 2, but prior to CDR 1, then the response force has a probability of 0.8 of defeating the adversary and foiling the attack.
- *Target Valuations* – Each target is assigned a value indicating the relative consequence if it were successfully attacked. The values chosen are:
    - Tower Target Valuation = 2
    - Switchyard Target Valuation = 1.

Defender Upgrades

The security upgrades we consider include both design changes and security measures that can be installed after construction. While a single budget applies to all upgrades in this example, our model's formulation is easily modified to categorize upgrades into security by design and operational security with separate budgets.

We select seven possible upgrades for this demonstration. Each upgrade imposes one or more of four possible effects on the network: reduce response time of the security force; decrease nondetection probability across one or more arcs; increase travel time across one or more arcs; and, increase probability of the response force defeating the adversary. A notional cost is assigned to each of the security upgrades. Again, cost values are only for illustrative purposes. The seven upgrades are as follows:

More Secure Location of Towers: Locate the tower and all its components within the protected area instead of the limited area. This upgrade forces the adversary to pass through an additional layer of security within the facility, thereby reducing his overall chance of nondetection and increasing his travel time. Specifically, if the towers are located within the protected area, then an additional-travel arc crossing the perimeter intrusion detection and assessment system (PIDAS) and traversing the protected area is introduced, as shown in Figure 4. This arc reduces the adversary's chance of nondetection en route to the tower target by 30%. A similar arc affects egress from the tower.

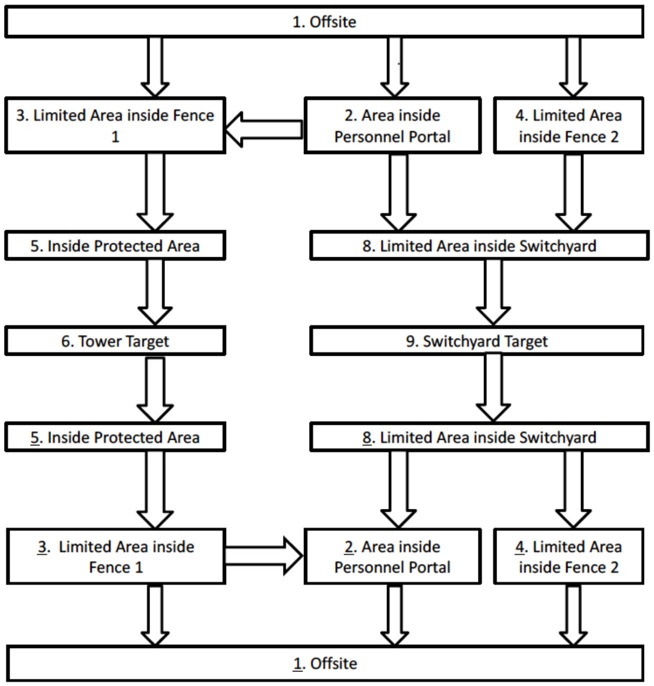

1. Offsite
3. Limited Area inside Fence 1
2. Area inside Personnel Portal
4. Limited Area inside Fence 2
5. Inside Protected Area
8. Limited Area inside Switchyard
6. Tower Target
9. Switchyard Target
5. Inside Protected Area
8. Limited Area inside Switchyard
3. Limited Area inside Fence 1
2. Area inside Personnel Portal
4. Limited Area inside Fence 2
1. Offsite

Figure 4. Mirrored network representation of tower relocation

System Redundancy: Introduce two identical cooling towers (and associated components) as well as two sets of switchyards to the baseline case. The redundant towers and switchyards are located on opposite sides of the limited area, as shown in Figure 5. This upgrade leads to two general attack strategies: the adversary may disable just one of the two redundant components at one-half the consequence of the baseline case (i.e., 0.5 per switchyard and 1 per tower), or he may disable the entire system (both towers or both switchyards) at the same consequence as the baseline case. This upgrade causes an increase in the travel time and a decrease in nondetection probability in disabling the entire system, as the adversary must now disable two systems to achieve an equivalent consequence. The mirrored network representation with system redundancy is outlined in Figure 6

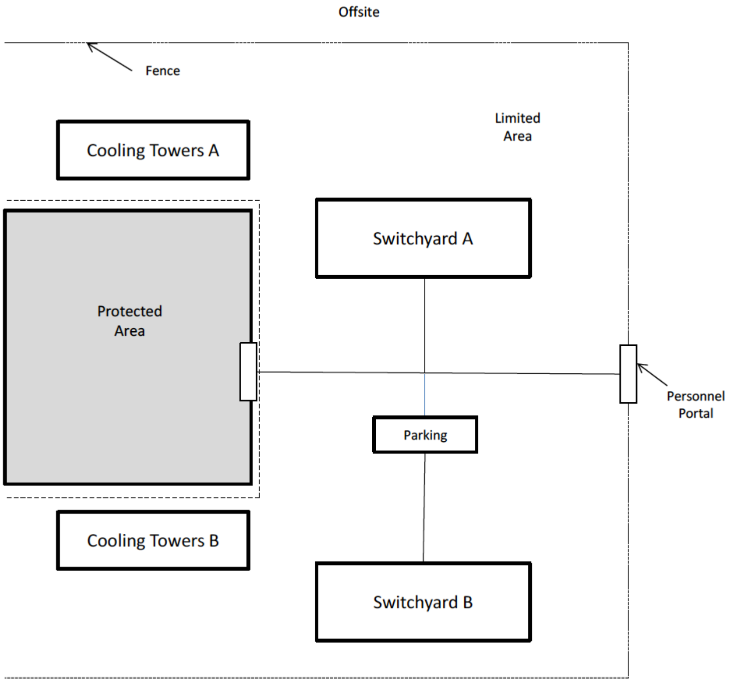


Figure 5. Conceptual depiction of system redundancy

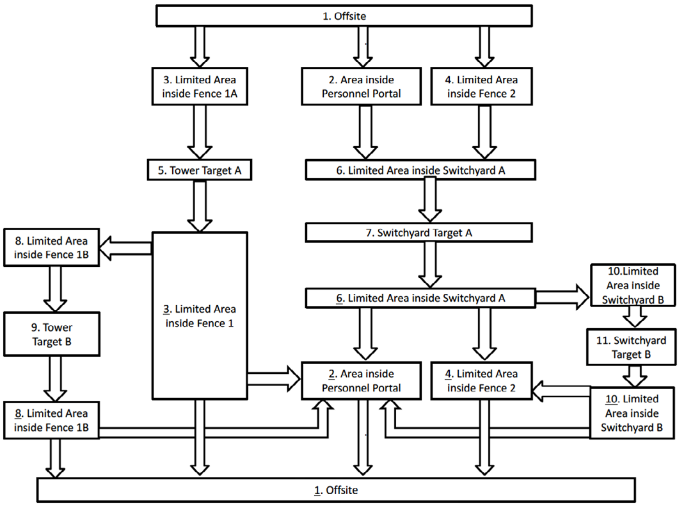

1. Offsite
3. Limited Area inside Fence 1A
2. Area inside Personnel Portal
4. Limited Area inside Fence 2
5. Tower Target A
6. Limited Area inside Switchyard A
7. Switchyard Target A
8. Limited Area inside Fence 1B
3. Limited Area inside Fence 1
6. Limited Area inside Switchyard A
10.Limited Area inside Switchyard B
9. Tower Target B
11. Switchyard Target B
2. Area inside Personnel Portal
4. Limited Area inside Fence 2
10. Limited Area inside Switchyard B
8. Limited Area inside Fence 1B
1. Offsite

Figure 6. Network representation of system redundancy

Structural Barriers: Introduce a delay in the vicinity of the tower by installing a concrete maze of walls. This investment affects the arcs leading to and from the cooling tower(s) in Figure 3 and the adversary requires twice the amount of time to complete his attack at the tower target compared to the baseline case. This investment does not affect nondetection probabilities.

Increase Detection: Provide additional search equipment and stationed guards in the limited area. This upgrade decreases the chance of nondetection by 20% on all arcs between node pairs (2,3), (2,6), and (4,6) in Table 1.

Increase Travel Time: Increase the height of the fences surrounding the limited area. By increasing the height, we force the adversary to climb to enter the limited area without using the personnel portal. This upgrade increases travel time by 25% on all arcs between node pairs (1,3) and (1,4) in Table 1.

Decrease Response Time: Reduce the time required for the response force to intercept the adversary upon detection from 70 to 50 (sec.).

Response Force Strength: Bolster the strength of the response force, increasing the force's probability of defeating the adversary upon interception. Specifically, the baseline probability of 0.8 when inside CDR 2, but outside CDR 1, increases to 0.9, and the baseline probability of 0.9 when outside CDR 2 increases to 0.95.

Table 2 provides a summary of the costs and effects of each upgrade. The costs should be interpreted in a relative sense.

Table 2. Summary of upgrade cost and effects Results and Discussion

Upgrade ID	Cost	Impact
A	$$	Move tower inside of PIDAS: add a node and arc on either side of tower target (in series), each with nondetection probability of 70%.
B	$$$$	Build redundant cooling tower and switchyard, each with half the consequence. Adversary has option to attack both sides by traversing additional arcs in the system.
C	$$	Multiply travel time by two for arcs on either side of Tower target.
D	$$	Reduce nondetection probability by 20% for all arcs between nodes (2,3), (2,6), and (4,6).
E	$$$	Increase travel time by 25% for all arcs between nodes (1,3) and (1,4).
F	$	Reduce response time by 20 seconds.
G	$	Increase defeat probability from 0.8 (inside CDR 2, outside CDR 1) and 0.9 (outside CDR 2) to 0.9 and 0.95, respectively.

Expected Consequences versus Budget

This section presents the results of the demonstration problem, using the parameters and potential upgrades defined above. We begin with the baseline network (budget *B* = 0) and tabulate defender investments and adversary behavior as the budget increases. Figure 7 displays the adversary's optimal path in the baseline problem. For Figures 7 through 10, the adversary's chosen (optimal) path is shown in gray, and dotted lines indicate where the adversary first reaches CDR 1 and CDR 2. Note that in many cases, the two CDRs are coextensive.

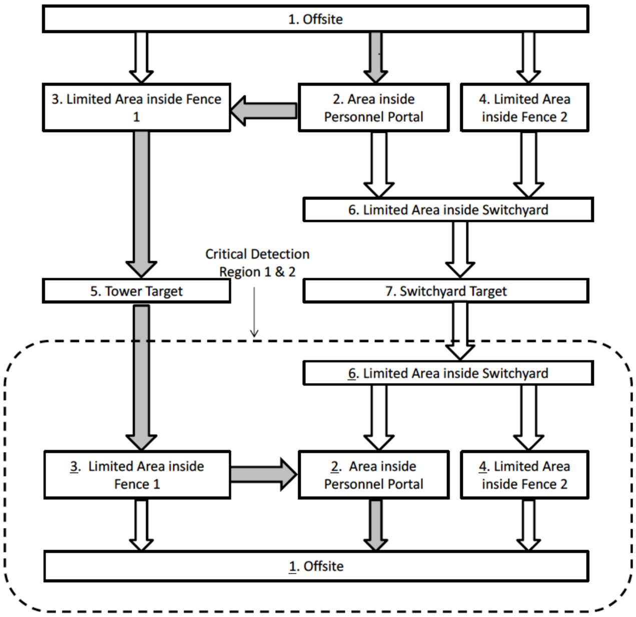

1. Offsite
3. Limited Area inside Fence 1
2. Area inside Personnel Portal
4. Limited Area inside Fence 2
6. Limited Area inside Switchyard
Critical Detection Region 1 & 2
5. Tower Target
7. Switchyard Target
6. Limited Area inside Switchyard
3. Limited Area inside Fence 1
2. Area inside Personnel Portal
4. Limited Area inside Fence 2
1. Offsite

Figure 7. Adversary path with a budget of B = 0

Figure 7 shows the adversary attacks the cooling tower, yielding an expected consequence of 0.96 (target consequence = 2, adversary's chance of success = 0.48). The two CDRs begin at the same location in the baseline case because the time-to-escape outside of the CDRs exceeds 100 seconds, and the time-to-escape within the CDRs is below 70 seconds, which satisfies conditions that defined both CDRs. No budget has been given to the defender, and so the game has not begun.

When the budget grows to *B* = 1, the defender implements upgrade G, strengthening the response force's defeat probability. This reduces the expected consequence by 8% and does not affect the adversary's pathway through the facility. Figure 8 shows the effect of increasing the budget to *B* = 2. The defender can now afford upgrade A, placing the cooling towers in the more secure protected area. The defender switches from implementing upgrade G to implementing upgrade A, which causes the nondetection probability to decrease and expands the CDRs by increasing the delay time on all arcs leading to the tower target. This causes the adversary to attack the switchyard, as can be seen in Figure 8, and reduces the expected consequence by 31% compared to the baseline facility.

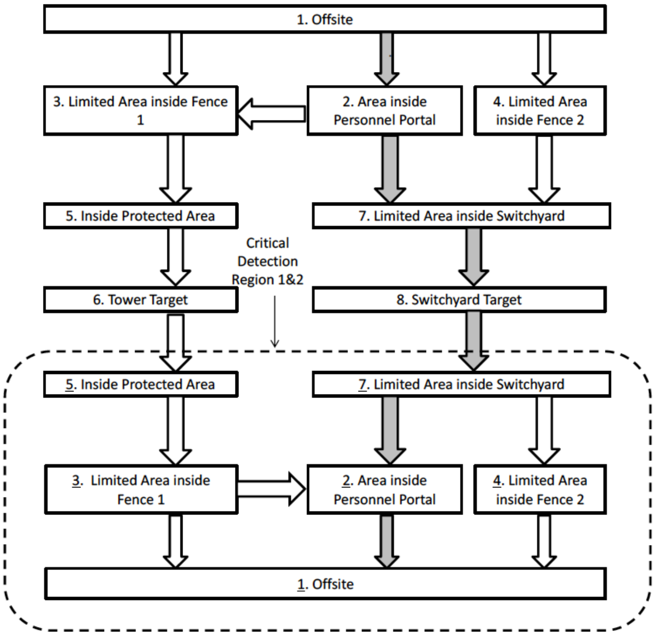

1. Offsite
3. Limited Area inside Fence 1
2. Area inside Personnel Portal
4. Limited Area inside Fence 2
5. Inside Protected Area
7. Limited Area inside Switchyard
Critical Detection Region 1&2
6. Tower Target
8. Switchyard Target
5. Inside Protected Area
7. Limited Area inside Switchyard
3. Limited Area inside Fence 1
2. Area inside Personnel Portal
4. Limited Area inside Fence 2
1. Offsite

Figure 8. Adversary path with a budget of B = 2

At *B* = 4, the defender still implements upgrade A to secure the cooling tower target, but also implements upgrades G and F, which defend both targets by strengthening the response force. When the defender's budget grows to *B* = 5, the defender chooses upgrades B and G. Upgrade B changes the layout of the facility by building redundant systems for each target, as can be seen in Figure 9. The defender can afford upgrade B at a budget of 4 but only finds the upgrade superior to other options once he can also afford to implement upgrade G, strengthening the response force's defeat probability.

At *B* = 5, the adversary attacks both cooling towers, even though he has the option of attacking only one at half of the payoff, as before. Because upgrade B changes the layout of the facility, the adversary's nondetection probability along the new arcs he must traverse to attack the second tower is less than 50%, and the payoff he receives if successful is 2 units (as opposed to 1 unit if he attacks just one tower). This suggests that it would not be in the adversary's best interest to attack the second tower in any situation. However, because the adversary has a small chance of defeating the response force, his chance of a successful attack on the second tower (by evading or defeating the defender) is slightly above 50%. The defender's investment strategy causes the consequence of the adversary's options to be nearly equal. There is a synergy between the design change (adding redundancy) and the operational upgrade (strengthening the response force). Redundancy increases the likelihood that an adversary seeking to disable both systems must face the response force, increasing the importance of the force's strength.

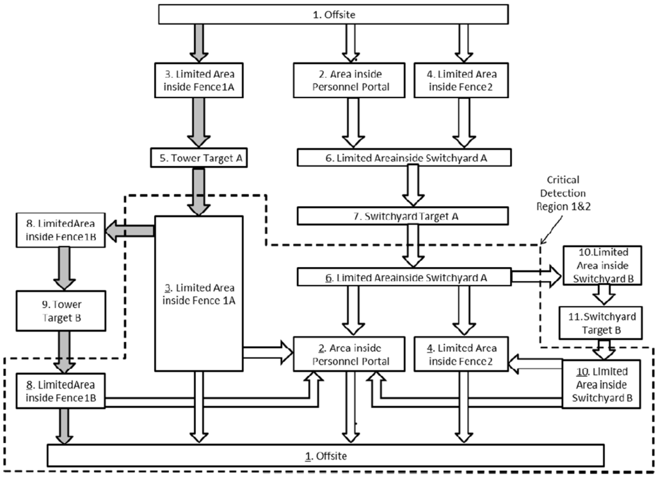

1. Offsite
3. Limited Area inside Fence1A
2. Area inside Personnel Portal
4. Limited Area inside Fence2
5. Tower Target A
6. Limited Areainside Switchyard A
Critical Detection Region 1&2
7. Switchyard Target A
8. LimitedArea inside Fence1B
10.Limited Area inside Switchyard B
6. Limited Areainside Switchyard A
9. Tower Target B
3. Limited Area inside Fence 1A
11.Switchyard Target B
2. Area inside Personnel Portal
4. Limited Area inside Fence2
10. Limited Area inside Switchyard B
8. LimitedArea inside Fence1B
1. Offsite

Figure 9. Adversary path with a budget of B = 5

As the budget grows further, the defender chooses investments that reduce the expected consequence of the adversary's optimal path; this yields a family of options with similar expected consequence, which in turn causes the adversary to switch targets and pathways multiple times, as several attack options become equally undesirable. In our example, the adversary switches to attacking both switchyard targets when *B* = 6, then to attacking only one cooling tower when *B* = 10, and then again to attacking both switchyards when *B* = 13.

At *B* = 10, the combination of upgrade F, along with the layout changes induced by upgrades A and B, causes the two CDRs to differ, as seen in Figure 10. Implementation of upgrade F, which reduces response time, and upgrades A and B, which reconfigure the facility layout, cause outbound nodes 5, 8, 10, and 12 to move inside CDR 2 while remaining outside CDR 1. If the adversary is detected while traveling to these nodes, he faces a battle with a faster-acting response force, whereas at lower budget levels he would have escaped. Since the nodes are inside CDR 2, though, the force has little time to prepare for the battle, and hence faces a reduced chance of defeating the adversary.

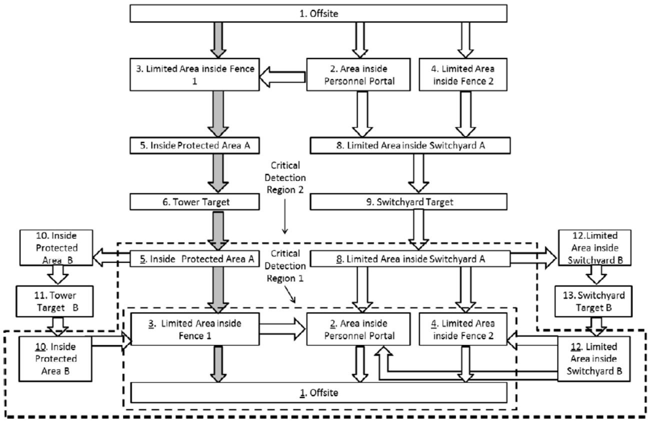

1. Offsite
3. Limited Area inside Fence 1
2. Area inside Personnel Portal
4. Limited Area inside Fence 2
5. Inside Protected Area A
8. Limited Area inside Switchyard A
Critical Detection Region 2
6. Tower Target
9. Switchyard Target
10. Inside Protected Area B
5. Inside Protected Area A
Critical Detection Region 1
8. Limited Area inside Switchyard A
12.Limited Area inside Switchyard B
11. Tower Target B
13. Switchyard Target B
3. Limited Area inside Fence 1
2. Area inside Personnel Portal
4. Limited Area inside Fence 2
10. Inside Protected Area B
12. Limited Area inside Switchyard B
1. Offsite

Figure 10. Adversary path with a budget of B = 10

Compared to the baseline facility, expected consequence reduces by 77% at budgets of *B* = 13 and higher, as the defender adopts all upgrades except for upgrade C. Given the numerical values chosen for our demonstration case, this upgrade does not improve expected consequence at any budget level. Upgrade C places a concrete maze outside all cooling tower target components, which causes an attack on the tower to take twice as long. Since this upgrade increases travel time on a node that is never within the CDR, the travel time for this node is irrelevant to our survival-oriented adversary. If detected early in his attack, the adversary will face the response force with certainty. Because this upgrade has no effect on the nondetection probability or CDR location, the adversary's attack is unaffected by this upgrade on any path through the facility.

Figure 11 summarizes the expected consequence versus budget up to *B* = 15, when the defender can implement all available upgrades. Table 3 summarizes the upgrades implemented for each budget. With this data, cost-benefit analyses can be performed on the upgrade options. For example, the efficient frontier illustrates that there are generally diminishing returns as the budget grows, but we see significant drops in expected consequence at specific budgets, notably *B* = 2, 5, and 8. At these budget levels, the defender can first afford a particularly effective upgrade or synergistic set of upgrades.

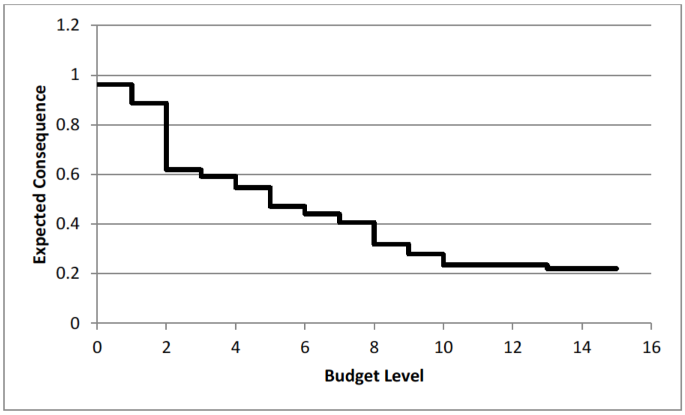


Figure 11. Efficient frontier

Table 3. Summary of results for each budget level

Budget	Expected Consequence	Solution (packages to purchase)	Path taken by Adversary
0	0.962	None	Tower
1	0.887	G	Tower
2	0.619	A	Switchyard
3	0.592	A,G	Switchyard
4	0.546	A,F,G	Switchyard
5	0.471	B,G	Tower (2)
6	0.441	A,B	Switchyard (2)
7	0.406	A,B,G	Switchyard (2)
8	0.318	A,B,D	Switchyard (2)
9	0.278	A,B,D,G	Switchyard (2)
10-12	0.235	A,B,D,F,G	Tower (1)
13-15	0.22	A,B,D,E,F,G	Switchyard (2)

Sensitivity Analysis

We conduct sensitivity analyses to exemplify use of the model as a security measure design-and-costing tool. We first explore the attractiveness of upgrade B, a design change that introduces redundant cooling tower and switchyard systems. We vary the cost of upgrade B from 1 up to 12 units, and at each cost we use model (1) to determine the smallest budget level at which upgrade B becomes attractive. The results are shown in Figure 12. Because upgrade B has a large effect, when its cost is low, the upgrade is implemented as soon as the defender can afford it, but at a cost of 4 units, as we have seen, the upgrade is not implemented until B = 5. When the cost of upgrade B grows to 5 units, other combinations of upgrades are competitive. In particular, synergistic sets that include upgrade A (cost of 2 units) are implemented in lieu of upgrade B at these budget levels. In addition, the combination of upgrades D, F, and G, which cost a total of 4 units, compete as upgrade B becomes more expensive. At a budget of B = 7, the defender forgoes B to implement A, D, F, and G only if upgrade B costs more than 5 units. At B = 8, the defender now finds the combination of upgrades A and B to be favorable even if B costs up to 6 units. However, at B = 9, the defender can afford to implement the synergistic combination of upgrades A D, E, F, and G, so that the defender's willingness to pay for upgrade B *drops* from 6 units to 5.

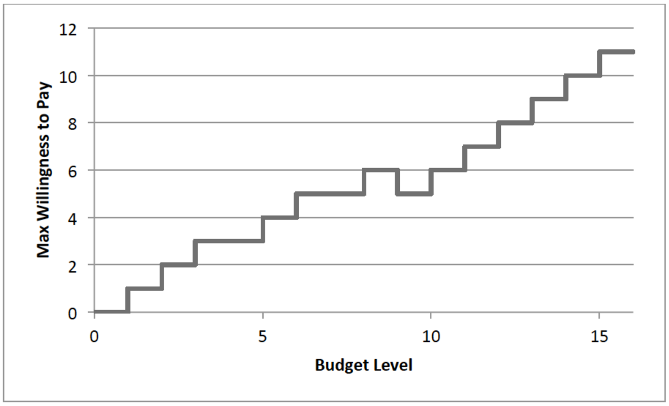


Figure 12. Sensitivity analysis on the attractiveness of upgrade B

Next we vary the effectiveness of upgrade D. In our reference case, this upgrade decreases the nondetection probability by 20% on a subset of arcs in the network. Figure 13 shows the change in the efficient frontier as the effectiveness of upgrade D varies. In all cases shown (10%, 20%, and 30% decrease in nondetection probabilities), D is implemented at $B \geq 8$. However, increasing the effectiveness of upgrade D from 10% to 20% has a larger effect than from 20% to 30%. Significantly, strengthening upgrade D beyond the 30% decrease in nondetection probability has no further effect on the efficient frontier because this decrease suffices to deter the adversary from traversing any arc upon which upgrade D applies. This reveals that overinvesting in improving the performance of upgrade D — say, by adding further guards or cameras — would be wasteful in the context of our model.

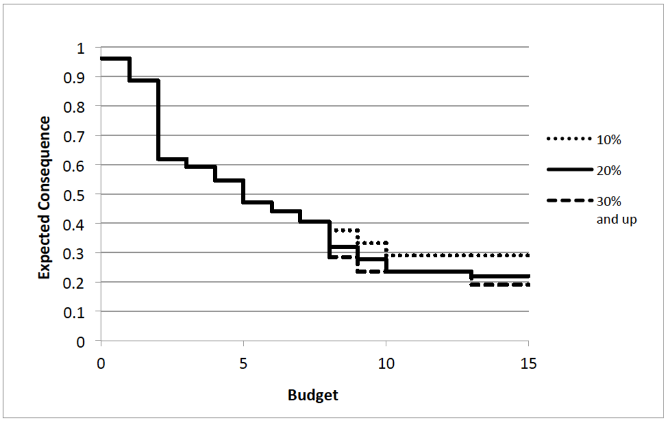


Figure 13. Sensitivity analysis on the strength of upgrade D

Our final analysis investigates how the valuation of the targets affects the upgrade investment portfolio. For this, we fix B = 4 and examine three sets of optimal upgrades. For each set, we vary the relative target values and plot that against expected consequence at budget B = 4, as shown in Figure 14. At our nominal target values (tower = 2, switchyard = 1), the consequence ratio is 1/3 and the defender implements upgrades A, F, and G. At any consequence ratio, the curve in Figure 14 with the lowest expected consequence is the optimal package of upgrades. The adversary's choice of target can be inferred from the line's slope; if the expected consequence is decreasing, the adversary targets the switchyard, and when the expected consequence increases, the adversary targets the cooling tower.

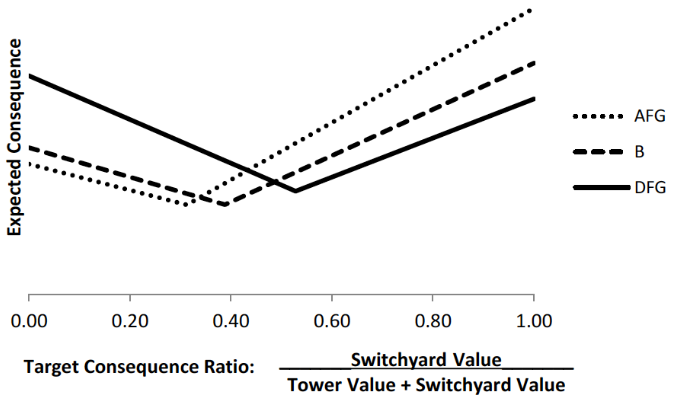


Figure 14. Sensitivity analysis on the values assigned to targets and the solutions implemented as a result

The objective of this sensitivity analysis is to quantify the degree to which an investment portfolio is suboptimal at any particular point on the horizontal axis. For instance, if we assume the value of the switchyard is 40% of the total value of both targets, then upgrade B is optimal. However, if the value of the switchyard is just 20% of the total, model (1) suggests implementing upgrades A, F, and G. In this case, though, the difference in expected consequence between the two upgrade packages is small.

On the other hand, assuming the switchyard valuation is 30% of the total yields upgrades A, F, and G as optimal, but if the value of the switchyard actually exceeds 55% of the total, the A, F, and G package is significantly suboptimal. If we are unable to assess the relative value of the targets, Figure 14 suggests that upgrade B is an attractive option. Even though it is optimal for a relatively narrow range of valuations, it serves as an effective hedge against target value uncertainty.

Conclusion

We have presented an innovative approach to securing a nuclear facility, combining PPS development with a game-theoretic model. We have shown how this method enables analysis of security investment options without the user constraining the adversary to attack along specific pathways. The adversary is conservatively modeled as omniscient and rational, and our model allows the adversary to both sneak and race through the facility, with a chance of defeating a response force if his stealth is unsuccessful. In our demonstration case, the defender is provided a small set of security upgrades that included facility design upgrades, response force upgrades, and added security measures. A richer analysis of such a facility would include many more potential targets as well as further security upgrades, including both design changes and operational measures possibly as a two-stage resource allocation problem, with separate budgets for the design and operational stages. Another potential extension of our model would consider multiple types of adversaries, such as an opponent who only seeks to cause damage with no regard for escape. The payoff function could then be weighted by the likelihood that the eventual attacker would be survival-oriented versus survival-indifferent, and the investment portfolio would represent the optimal strategy for guarding against both types of opponents.

It is also possible to model a series of defensive investments made over time to replicate, for example, an annual budget for security upgrades. When the game is reformulated in this way, the defender cannot undo investments he had made at lower budget levels. Finally, not all defensive investments are best modeled as transparent to the attacker. For instance, the defender may install dummy as well as active video surveillance systems. An adversary may know where the systems are located but may not be aware which ones are active. A mixture of transparent and non-transparent defensive systems can be modeled via a combined Stackelberg-Cournot game.

Acknowledgments

This work was supported in part by the U.S. Department of Energy under Sandia National Laboratories contract number PO 1252537.

References

1. Gaukler, M., Li, C., Cannaday, F., Chirayath, S., and Ding, Y. 2011. Detecting Nuclear Materials Smuggling: Using Radiography to Improve Container Inspection Policies, *Annals of Operations Research*, 187:65–87.
2. Wein, L.M., Wilkins, A.H., Baveja, M., and Flynn, S.E. 2006. Preventing the Importation of Illicit Nuclear Materials in Shipping Containers, *Risk Analysis*, 26:1377–1393.
3. Boros, E., Fedzhora, L., Kantor, P.B., Saeger, K.J., and Stroud, P. 2009. Large Scale LP Model for Finding Optimal Container Inspection Strategies. *Naval Research Logistics*, 56:404–420.
4. Madigan, D., Mittal, S., and Roberts, F. 2007. Sequential

Decision Making Algorithms for Port of Entry Inspection: Overcoming Computational Challenges. *Proceedings of IEEE International Conference on Intelligence and Security Informatics* (ISI-2007), 1–7.

5. McLay, L.A., Lloyd, J.D., and Niman, E. 2011. Interdicting Nuclear Material on Cargo Containers Using Knapsack Problem Models, *Annals of Operations Research*, 187:185–205.
6. Stroud, P.D. and Saeger, K.J. 2003. Enumeration of Increasing Boolean Expressions and Alternative Digraph Implementations for Diagnostic Applications. *Proceedings Volume IV, Computer, Communication and Control Technologies,* 328–333.
7. Dimitrov, N.B., Michalopoulos, D., Morton, D.P., Nehme, M.V., Pan, F., Popova, E., Schneider, E.A., and Thoreson, G.G. 2011. Network Deployment of Radiation Detectors with Physics-Based Detection Probability Calculations, *Annals of Operations Research*, 187:207–228.
8. Nehme, M.V. 2009. Two-Person Games for Stochastic Network Interdiction: Models, Methods, and Complexities, Ph.D. thesis, University of Texas at Austin.
9. Morton, D.P., Pan, F., and Saeger, K.J. 2007. Models for Nuclear Smuggling Interdiction, *IIE Transactions on Operations Engineering*, 38:3–14.
10. Pan, F. and Morton, D.P. 2008. Minimizing a Stochastic Maximum-Reliability Path, *Networks*, 52:111–119.
11. Pan, F., Charlton, W., and Morton, D.P. 2003. Interdicting Smuggled Nuclear Material, *Network Interdiction and Stochastic Integer Programming*, D.L. Woodruff, ed., pp. 1–20. Kluwer Academic Publishers, Boston.
12. Atkinson, M.P., Cao, Z., and Wein, L.M. 2008. Optimal Stopping Analysis of a Radiation Detection System to Protect Cities from a Nuclear Terrorist Attack, *Risk Analysis*, 28:353–371.
13. Brashear, J.P. and Jones, J.W. 2010. Risk Analysis and Management for Critical Asset Protection (RAMCAP Plus), *Wiley Handbook of Science and Technology for Homeland Security*, 1–15.
14. National Research Council (NRC). Department of Homeland Security Bioterrorist Risk Assessment: A Call for Change. NRC, Washington, DC, 2008.
15. National Research Council (NRC). Review of the Department of Homeland Security's Approach to Risk Analysis. NRC, Washington, DC, 2010.
16. Brown, G. and Cox, A. 2011. How Probabilistic Risk Assessment can Mislead Terrorism Risk Analysis, *Risk Analysis*, 31:196–204.
17. Cox, A. 2008. Some Limitations of "Risk = Threat *x* Vulnerability *x* Consequence" for Risk Analysis of Terrorist Attacks, *Risk Analysis*, 28:1749–1761.
18. Cox, A. 2009. Improving Risk-Based Decision Making for Terrorism Applications, *Risk Analysis*, 29:336–341.
19. Golany, B., Kaplan, E.H., Marmur, A., and Rothblum, U.G. 2009. Nature Plays with Dice – Terrorists Do Not: Allocating Resources to Counter Strategic Versus Probabilistic Risks, *European Journal of Operational Research*, 192:198–208.
20. Ward, R. and Schneider, E. 2012. Incentivizing Timely Detection: Game Theoretic Modeling of Trade-Offs, *Transactions of the American Nuclear Society*, 106.
21. Brown, G.G., Carlyle, W.M., Harney, R., Skroch, E., and Wood, R.K. 2009. Interdicting a Nuclear-Weapons Project, *Operations Research*, 57:866–877.
22. Harney, R., Brown, G.G., Carlyle, W.M., Skroch, E., and Wood, R.K. 2006. Anatomy of a Project to Produce a First Nuclear Weapon, *Science and Global Security*, 14:163–182.
23. Salmeron, J., Wood, R.K., and Baldick, R. 2004. Analysis of Electric Grid Security Under Terrorist Threat, *IEEE Transactions on Power Systems*, 19(2):905–912.
24. Salmeron, J., Wood, R.K., and Baldick, R. 2009. Worst-Case Interdiction Analysis of Large-Scale Electric Power Grids, *IEEE Transactions on Power Systems*, 24(1):96–104.
25. Berry, J., Hart, W.E., Phillips, C.A., Uber, J.G., and Watson, J. 2006. Sensor Placement in Municipal Water Networks with Temporal Integer Programming Models, *Journal of Water Resources Planning and Management*, 132(4):218+.
26. Berry, J., Carr, R.D., Hart, W.E., Leung, V.J., Phillips, C.A., and Watson, J. 2009. Designing Contamination Warning Systems for Municipal Water Networks Using Imperfect Sensors, *Journal of Water Resources Planning and Management*, 135(4):253+.
27. Murray, R., Haxton, T., Janke, R., Hart, W.E., Berry, J., and Phillips, C.A. 2010. Sensor Network Design for Drinking

Water Contamination Warning Systems: A Compendium of Research Results and Case Studies using the TEVA-SPOT Software. Technical Report EPA/600/R-09/141, National Homeland Security Research Center, Office of Research and Development, U.S. Environmental Protection Agency.

28. Watson, J., Murray, R., and Hart, W.E. 2009. Formulation and Optimization of Robust Sensor Placement Problems for Drinking Water Contamination Warning Systems, *Journal of Infrastructure Systems*, 15(4):330+.

29. Armbruster, B., Smith, J.C., and Park, K. 2007. The Optimization of Packet Filter Placements to Combat Distributed Denial of Service Attacks, *European Journal of Operational Research*, 176:1283–1292.

30. Paruchuri, P., Pearce, J.P., Marecki, J., Tambe, M., Ordonez, F., and Kraus, S. 2008. Playing Games for Security: An Efficient Exact Algorithm for Solving Bayesian Stackelberg Games. Proceedings of the 7th International Joint Conference on Autonomous Agents and Multiagent Systems, volume 2, pp. 895–902.

31. Alderson, D.L., Brown, G.G., Carlyle, W.M., and Wood, R.K. 2011. Solving Defender-Attacker-Defender Models for Infrastructure Defense, *Operations Research, Computing, and Homeland Defense,* Wood, R.K. and Dell, R.F., eds., pp. 28-49. INFORMS, Hanover, MD.

32. Brown, G.G., Carlyle, M., Salmeron, J., and Wood, R.K. 2006. Defending Critical Infrastructure, *Interfaces*, 36:530–544.

33. Dimitrov, N.B. and Morton, D.P. 2012. Interdiction Models and Applications, *Handbook of Operations Research for Homeland Security*, J.W. Herrmann, Springer.

34. Garcia, M.L. 2001. *The Design and Evaluation of Physical Protection Systems*. Boston: Butterworth-Heinemann.

35. Property arcs were not present in the previous example network. A travel time of 60 seconds is used for all property arcs.

Process-Informed Safeguards Strategy for a Pyroprocessing Facility

By T. R. Riley, C. L. Pope, and R. W. Benedict

Abstract

Pyroprocessing is a nonaqueous spent nuclear fuel recycling technique. If implemented on a commercial scale, longstanding safeguards approaches used to satisfy IAEA requirements in traditional aqueous-based processes may be unworkable. To aid in testing elementary safeguards strategies, two new tools were developed: (1) the Pyroprocessing Safeguards Performance Model, a MATLAB/Simulink simulation of plant operations capable of calculating inventory differences for a specified balance period as well as sensitivity studies of detection measurements, and (2) the Safeguard Hazards Matrix, a risk matrix developed using the calculated inventory difference and probability to detect diversion of one significant quantity to represent the risk of diversion within a reference facility. Using both tools, four strategies were evaluated: (1) the black box, (2) conventional, (3) process informed, and (4) process informed with rejection sampling. An empirically derived quality factor was also developed to provide a measure of the spread of the calculated inventory difference over the course of operation. Process information, specifically mass balance data from a mass tracking system, significantly reduces the safeguards risk in a pyroprocessing facility.

Keywords: pyroprocessing, spent fuel, PSPM, safeguards

Introduction

Pyroprocessing of fast reactor spent fuel has been demonstrated on an engineering scale.[1] Current technology demonstrations with throughputs of ~10 MTiHM/yr relied on low throughputs to meet safeguards requirements; however, commercial facilities with throughputs of 100 MTiHM/yr and greater will not be able to meet safeguards requirements using the same approach followed on an engineering scale. For greater throughput facilities, new approaches to meeting safeguards requirements will be needed.[2] To aid in testing strategies, the Pyroprocessing Safeguards Performance Model (PSPM) and the Safeguard Hazards Matrix were developed.

Material Accountancy Terms

Terms used in Material Control and Accountability (MC&A) regulations vary by regulator; for clarity, key terms used in this paper are defined here. Special nuclear material tracking throughout a facility utilizes material balance areas (MBAs) to account for and monitor material. A material inventory difference (ID) is defined as inputs plus starting inventory minus ending inventory and outputs, also known as material unaccounted for (MUF).

$$\text{ID} = \text{Inputs} + \text{Beginning Inventory} - \text{Outputs} - \text{Ending Inventory} \qquad (1)$$

A significant quantity (SQ) is the amount of fissile material required to produce an improvised nuclear device; 75 kg of low enriched uranium or 8 kg of Pu.[3] To ensure that the ID is less than 1 SQ, the standard error in inventory difference (SEID) is introduced, also known as m_{ud}. SEID is a summation of the variances introduced by each ID measurement. A measurement system must also have a 95% detection probability to detect a diversion of an SQ and a 5% false alarm probability. Operating experience from bulk handling facilities (such as reprocessing plants) has shown ID to be a standard normal distribution, as described by Equation 2.

$$f(x) = \frac{1}{\sqrt{2\pi}} e^{\frac{(1-x)^2}{2}} \qquad (2)$$

Integration of Equation 2, to calculate the desired detection probability of 95%, yields 1.65. This *x* value corresponds to both the detection probability and false alarm probability requirements provided by the International Atomic Energy Agency (IAEA). Assuming a loss of 1 SQ over 1 year, testing for loss only (not gain), and setting the false alarm probability to 0.05, the alarm probability is 0.95, provided Equation 3 holds true.

$$SEID \leq \frac{\text{SQ}}{3.3} \qquad (3)$$

The factor of 3.3 arises from double use of the value 1.65, which corresponds to both the 0.05 false alarm probability and the 0.95 alarm probability.[4] To assure detection of a loss of 1 SQ, Equation 3 must hold true.[4] For Pu and low enriched uranium, SEID must be less than 2.424 and 22.7 kg, respectively.[3]

ID and SEID are calculated once for a specific inventory period, to determine if material diversion may have occurred. IAEA regulations require the timely detection of the loss of 1 SQ of material within 30 days.

Conventional Safeguards

Safeguards requirements applied to aqueous reprocessing facilities fundamentally rely on measurement uncertainty and inventory frequency. As facility throughput demands increase, improvements in measurement uncertainty or more frequent inventory or combinations of these must occur. The problem is exacerbated when the input material transitions from light water reactor (LWR) spent fuel to fast reactor spent fuel because the fissile content of fast reactor spent fuel is higher than that of LWR spent fuel. For example, Table 1 illustrates safeguards data representative of a commercial aqueous reprocessing facility.[5] As seen in Table 1, to meet IAEA detection requirements, the inventory period must be shortened significantly or the total measurement uncertainties (random and systemic combined) need to be less than 0.1%.

The safeguards challenge is more complicated in a pyroprocessing facility. The root of the safeguards challenge in a pyroprocessing facility centers on the lack of a starting point in the process where an accurate (<1% uncertainty) input mass measurement can be made without significant measurement technology development. To date, pyroprocessing facilities have been able to meet safeguards requirements with relatively low throughputs; however, a commercial facility will not be economical at these throughputs.

Reference Facility

To explore the safeguards challenge associated with commercial-scale pyroprocessing of LWR spent fuel, a reference pyroprocessing facility was assumed to have an annual spent nuclear fuel throughput of 100 MTiHM/yr. The facility design was based on reprocessing fuel assemblies that have an initial enrichment of 4.5% and burnup of ~50 GWd/MTiHM. The assemblies were discharged from the reactor for ~10 years before being processed. Figure 1 provides the process flow assumed for the pyroprocessing facility.[6] Figure 2 contains a hypothetical hot cell layout for the reference facility,[7] including entrance and exit pathways from the MBA.

Table 1. Commercial-scale reprocessing facility summary

Parameter	LWR Application	Fast Reactor Application
Heavy metal capacity	800 MTiHM/yr	250 MTiHM/yr
Pu content (% HM)	1.33%	6–20%
Pu mass flow (max)	36 kg/day	50–170 kg/day
Inventory period	30 days	30 days
Input Pu mass uncertainty	0.70%	0.70%
SEID	7.86 kg	10.92–37.13 kg
Altered inventory period to achieve SEID goal	9.2 days	6.6–2.0 days
Altered input Pu uncertainty to achieve SEID goal	0.10%	Not plausible

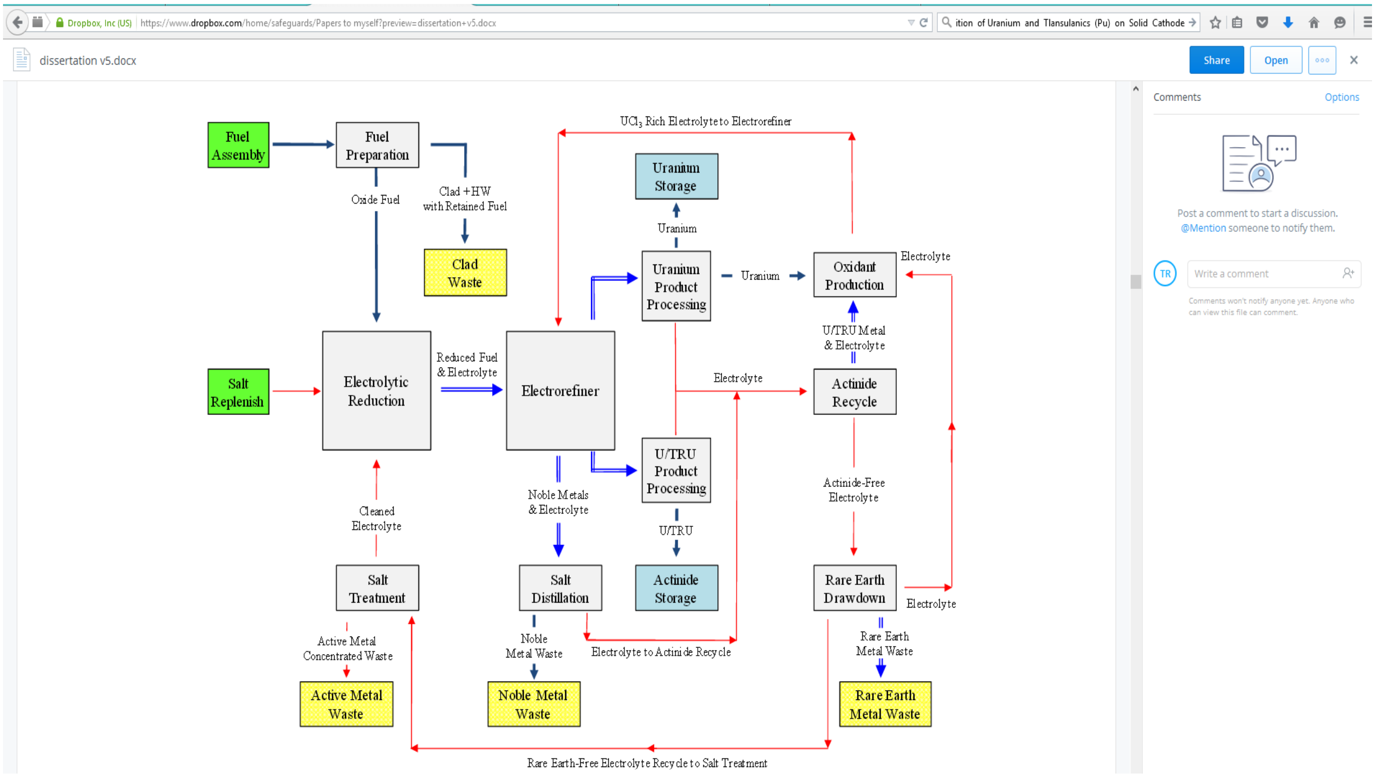

Dropbox, Inc (US) https://www.dropbox.com/home/safeguards/Papers to myself?preview=dissertation+v5.docx
ition of Uranium and Tlansulanics (Pu) on Solid Cathode
dissertation v5.docx
Share
Open
Comments
Options
Post a comment to start a discussion.
@Mention someone to notify them.
TR
Write a comment
Comments won't notify anyone yet. Anyone who can view this file can comment.
Fuel Assembly
Fuel Preparation
Oxide Fuel
Clad +HW with Retained Fuel
Clad Waste
UCl3 Rich Electrolyte to Electrorefiner
Uranium Storage
Uranium
Uranium Product Processing
Uranium
Oxidant Production
Electrolyte
U/TRU Metal & Electrolyte
Salt Replenish
Electrolytic Reduction
Reduced Fuel & Electrolyte
Electrorefiner
Electrolyte
Actinide Recycle
U/TRU Product Processing
Noble Metals & Electrolyte
U/TRU
Actinide-Free Electrolyte
Cleaned Electrolyte
Salt Treatment
Salt Distillation
Actinide Storage
Rare Earth Drawdown
Electrolyte
Active Metal Concentrated Waste
Noble Metal Waste
Electrolyte to Actinide Recycle
Rare Earth Metal Waste
Active Metal Waste
Noble Metal Waste
Rare Earth Metal Waste
Rare Earth-Free Electrolyte Recycle to Salt Treatment

Figure 1. Pyroprocessing process flow

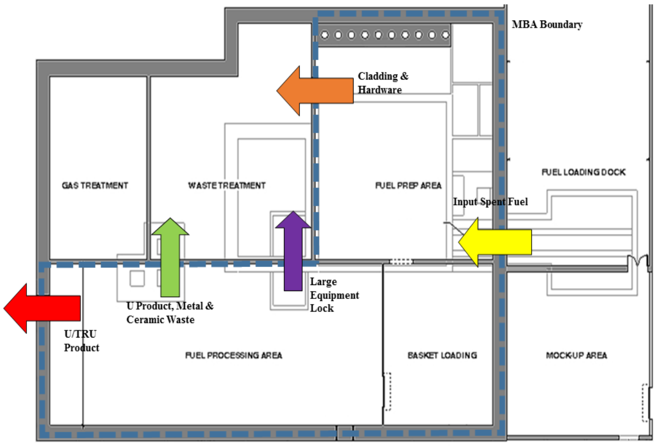


Figure 2. Reference pyroprocessing facility hot cell layout with entrance/exit pathways

Pyroprocessing has several areas of interest regarding safeguards application. The spent fuel receiving and storage area encompasses the storage capacity of the facility and houses the receiving equipment for spent fuel shipped from other sites. The air-atmosphere hot cell contains nondestructive assay (NDA) equipment used to verify the assembly contents to determine the Shipper/Receiver difference and provide the initial safeguard measurement of the key parameters of interest, namely the U^{235} and plutonium mass. Within this air cell, the assembly is disassembled and fuel pellets are transferred to the inert atmosphere process hot cell and loaded into Process Basket Modules (PBM). The fuel is then reduced to metal from its initial oxide form via electrolytic reduction in the electroreducer (ERed) and then moved to the electrorefiner (ERef).

The ERef contains a lithium chloride-potassium chloride (LiCl-KCl) salt where actinides, including transuranic elements (TRU), and some fission products form stable chlorides. A voltage is applied across the anode and cathode, which induces the electrotransport of the uranium onto cathode rods and the TRU deposits on separate cathodes.[8] The uranium metal dendrite deposits on the cathode rod and is transferred to a distillation furnace commonly referred to as a cathode processor. During the TRU electrotransport process, some uranium will codeposit, as well as a small fraction of rare earth elements (~0.1%). A U/TRU cathode is collected at the end of ERef processing. Due to U/TRU products' lower melting point, the salt and TRU metal are separated by density differences in a bottom pour furnace to produce a U/TRU ingot and salt stream for recycle. The purified ingots are then moved from the process cell to their respective storage locations, the U/TRU vault and a U storage area.

The adhering salts are collected, along with some salt from the ERef after three processing cycles. The salt's actinide composition is drawn down first. This is combined with uranium metal to produce the oxidant (UCl_3) needed to facilitate electrotransport in the ERef. Once the actinides are drawn down, the rare earth elements are drawn out of the salt. In the following step, the rare earth free salt is sent to a storage tank until another rare earth free salt batch is processed. This actinide and rare earth free salt has the active metals removed via salt crystallization. The cleaned salt is then recycled into the electrolytic reduction vessel.

An analytical laboratory is used to analyze material samples taken at designated key measurement points to confirm that no Special Nuclear Material (SNM) is being diverted and help resolve and detect differences. The samples are on the order of a few grams and are analyzed with destructive analysis (DA) and/or NDA techniques.

The processing and air hot cells make up a single MBA, whereas each storage area for U and TRU products and spent fuel awaiting processing has separate MBAs. The main processing MBA was selected to have a minimum number of pathways into or out of the cell; the blue dashed line in Figure 2 is the assumed MBA boundary for the facility — one input pathway and four exit pathways from the hot cells.

Pyroprocessing Safeguards Performance Model

The Pyroprocessing Safeguards Performance Model (PSPM)[7,9] is a MATLAB/Simulink[10] discrete event simulation model of the reference facility. The PSPM tracks material movements throughout the various processes within the facility and calculates the MBA's ID and SEID at the end of each inventory period. The PSPM contains simulated measurement points at each process, allowing the user to select which points to include in the calculation of the ID and SEID for the inventory period. Each process contains a simulated sensor that provides a random, normally distributed signal based on the average mass at that measurement point and a user-specified total measurement uncertainty (σ), combined random and systemic, for the device used. This is then output to the plant monitoring subsystem to simulate the response of sensors in the facility. Different safeguards strategies can be evaluated by choosing which sensors to include in the ID and SEID calculations.

Safeguards Strategies

The PSPM was used to investigate different safeguard approaches, with varying measurement techniques, to detect the loss of an SQ of SNM. Common to each of the strategies is the assumption of one MBA used to encompass both the processing and fuel preparation cells as shown in Figure 2. The equipment transfer lock is not included in this analysis, as use of this pathway would constitute an off-normal processing event, which is not considered by this work. It is, however, acknowledged that the transfer lock will need containment and surveillance measures to ensure SQs of material are not removed while components are transferred to and from the processing cell.

Four safeguard strategies, known as *levels*, were used to demonstrate the effectiveness of a risk matrix, described below, as a tool in safeguards evaluation. Each level builds on elements of the previous level to enhance the strategy.

The level 1 strategy consists of treating the facility as a black box, with only inputs and outputs considered. ID can be calculated as the transfers into the MBA minus the transfers out of the MBA, with no measure of the inventory within the facility. Figure 3 shows key measurement points (KMPs) with blue dots and the material measured at each point for this strategy. Level 1 is the reference or unmitigated case.

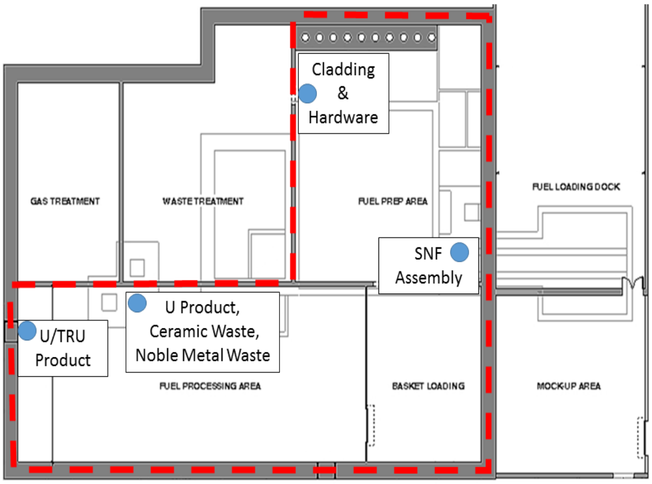


Figure 3. Level 1 key measurement points

Level 2 expands on the level 1 strategy by including measurements from storage locations of material. Using the PSPM, storage locations containing SNM at the end of each balance period were determined. Four storage locations were identified and incorporated into inventory measurement: storage of uranium to be sent to oxidant production, storage of containers of fuel pellets awaiting electroreduction (PBM store), a container of fuel pellets awaiting transfer to storage prior to electroreduction (PBM accum), and the salt collection tank. Figure 4 shows the KMPs of level 1 in blue and new level 2 KMPs in green with associated locations within the cell.

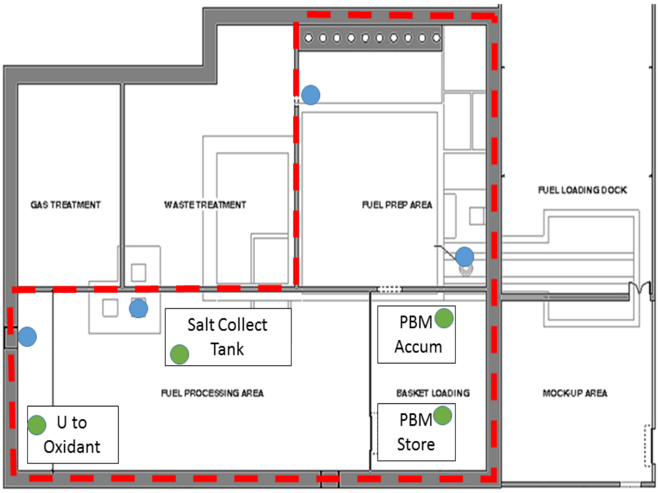


Figure 4. Level 2 key measurement points

For each location, the overall mass is reported along with the corresponding measurement uncertainty from the process model to the monitoring system. This strategy represents a conventional safeguards approach.

Level 3 integrates process data into level 2, a process-informed safeguards strategy. The process monitoring system, which can have the most impact on a safeguard system, is a detailed mass tracking system. With such a system, mass balances are used to weigh every item before and after it is processed by a unit or moved from one zone to another within the MBA. The MBA would be divided up into internal zones for each processing unit. Including process information in the safeguards strategy will require the mass tracking system to be available for both the operator and international inspectors. Traditionally, this stipulation has required two separate devices: one for the IAEA, and a second identical system for the operator. However, joint use systems have been implemented at the Rokasho-Mura Processing Plant in areas where two detectors are not possible. These systems provide independent and identical signals to each party that can be analyzed by each organization, with separate conclusions drawn.[11,12] Figure 5 shows the KMPs for level 1 and 2 in blue and green, respectively; level 3 KMPs are shown in yellow.

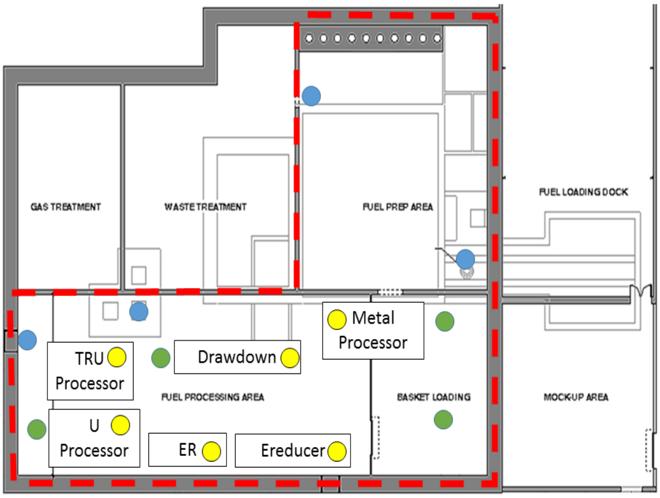


Figure 5. Levels 3 and 4 key measurement points

The balances are connected to a network that can store all vital information about a specific item, such as the starting weight when it entered a zone, the item's serial number, and the balance to be used. Verifying an item is the correct weight and serial number by two independent observers adds an additional layer of protection. The tracking system is also used to compare the item weight to its initial recorded weight. A system such as this was implemented at the Fuel Conditioning Facility (FCF) at Idaho National Laboratory and has been used for almost 20 years (with some upgrades from the original system installed in 1995) to handle over 35,000 fissile material transfers (as of 2006).[13]

A system like that of the FCF can provide information on the number of "in- process" items throughout the facility. For example, the number of processing containers in the ERed at the end of a balance period can be added to the inventory using a standard composition because the material has been tracked since entering as a fuel assembly. The composition would be a valid assumption because initial NDA/DA measurements on the input spent fuel assembly would identify anomalies. Once initially measured, the material would be tracked using the tracking system to record the processing vessel, container serial numbers, and a characteristic weight. This strategy adds safeguards information without forcing the facility to shut down for a balance closure each 30day period or less, as occurs in aqueous facilities. This is a necessary attribute of any pyroprocessing strategy because the process vessel with molten salt cannot be routinely emptied. In level 3, as implemented in the PSPM, only the holdup within a processing vessel is not measured, so the ID represents the holdup and random fluctuations from measurement uncertainties.

Level 4 applies rejection sampling to the input and output measurements determined in level 3; the same KMPs as in level 3 are used. The use of an integrated mass tracking system implies every item entering and exiting the MBA will be weighed, and only items within an accepted tolerance will be allowed to leave or enter the cell; anomalies will be rejected and will not be allowed into the cell without tripping an alarm. The PSPM determines a random mass from a normal distribution with a mean of the mass from the process model and a standard deviation of the measurement device for each group. However, if the sum of all these random measurements exceeds the tolerance of the mass balance, the item would be rejected. To illustrate this, assume an item is composed of three materials — a, b, and c — with corresponding average masses of 1, 2, and 3. Now assume the measurement device (i.e., NDA device) has a standard deviation of 10% for each individual material, while the mass balance has a tolerance of 0.1% for the total mass of the item. The average item mass is then 6; however, using random sampling for each material could result in an estimation of the item mass greater than the mass balance's tolerance. A MATLAB script was created to show the effect of rejection sampling for this case; the results in Table 2 were generated with 1 million simulated masses for each material.

Table 2. Rejection sampling effect

	No Rejection Sampling		Rejection Sampling	
Material	Mean	STD	Mean	STD
a	1.0002	0.1000	1.0000	0.0818
b	2.0001	0.1000	2.0001	0.0816
c	2.9999	0.1000	2.9999	0.0819
Total	6.0002	0.1732	6.0000	0.0104

The rejection sampling is invoked if the sum of a, b, and c is greater than or less than the mean ± 3*$s_{balance}$. If these conditions are true, the logic continues to generate random normally distributed pairs until the condition is false. Rejection sampling is only a benefit if the measurement device distributions have a greater uncertainty than the mass balance uncertainty. This technique results in an order of magnitude decrease in the standard deviation of the total mass of the item. Application of this to a safeguards system helps to reduce the spread of ID measurements and gain increased assurance from less-precise detection equipment (i.e., NDA or process monitoring devices) that diversion has not occurred.

Safeguards Hazards Matrix

The Safeguards Hazards Matrix (SHM) is adapted from nonreactor nuclear facility safety analysis techniques applied to Department of Energy (DOE) and Nuclear Regulatory Commission (NRC) regulated facilities. Both DOE and NRC regulated fuel cycle facilities conduct safety analysis using a risk matrix approach. A risk matrix is used to quantify the risk of accident sequences and to identify acceptable and unacceptable sequences. A risk matrix lists accident likelihood categories along the abscissa and accident consequence categories along the ordinate. The likelihood categories and consequence categories are assigned monotonically increasing positive integer values starting with the number 1. The multiplication product of these two integer values is called a risk index. Risk index values are used to fill the risk matrix elements. Based on the resulting risk index value, accident sequences are classified as either acceptable or not acceptable. In general, the risk matrix approach recognizes that low frequency, high consequence events are equally as unacceptable as high frequency, low consequence events.

In the SHM, diversion risk is determined as proportional to the amount of material unaccounted for (ID) and the probability to detect a loss of an SQ (see Figure 6). Using the PSPM, the limiting factor for an SQ of material is Pu, so only Pu requirements will be discussed further; however, the SHM could be applied to U with appropriate ID values. The limits for the *x*-axis bins were based on the requirement by DOE for SEID < 2 kg, while the others were the author's intuition. Risk bins 7–16 (grayed boxes) are deemed unacceptable risk, whereas bins 1–6 are acceptable. The risk of the safeguards approach can be decreased by increasing the probability of detection and/or decrease the ID. Of course, the bins can be shifted as desired. The idea here is to demonstrate a pathway for evaluating safeguards strategies rather than establishing definitive risk acceptance values.

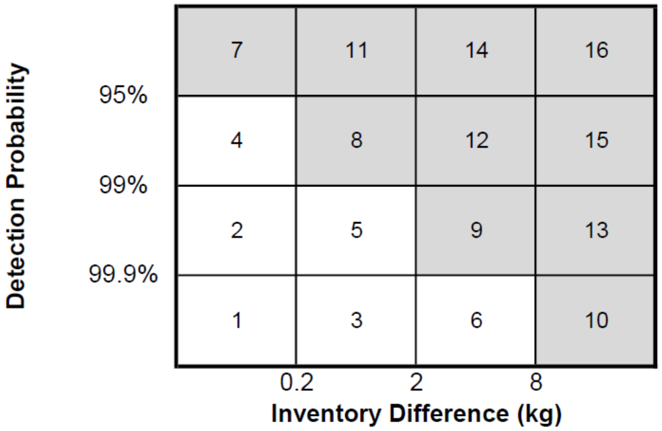


Figure 6. The Safeguards Hazards Matrix

The detection probability is calculated by solving for *x* in Equation 2 using a known SEID. The detection probability for loss of one SQ can be shown to be:

$$DP = \frac{\mathrm{erf}\left(\frac{Q}{2 * SEID * \sqrt{2}}\right) + 1}{2} \qquad (4)$$

In Equation 4, *Q* is the amount in kg of material representative of one SQ, *SEID* is the calculated SEID from the PSPM, and *DP* is the detection probability. As noted earlier, a factor of 2 in the error function arises from the assumption that the false alarm probability is also the same.

Results

The PSPM and SHM provide a testbed to evaluate potential safeguards approaches. A separate 1-year simulation of facility operation was conducted, with the PSPM, for levels 1 through 4. These simulations were each repeated 1,000 times with different random number seeds each time to provide a statistical variation to the ID and SEID calculations. An average ID and SEID were calculated as well as the standard deviation of these averages. Several strategies with varying measurement uncertainties were simulated, using the PSPM and plotted in Figure 7; a summary of the input parameters corresponding to each case is included in Table 3.

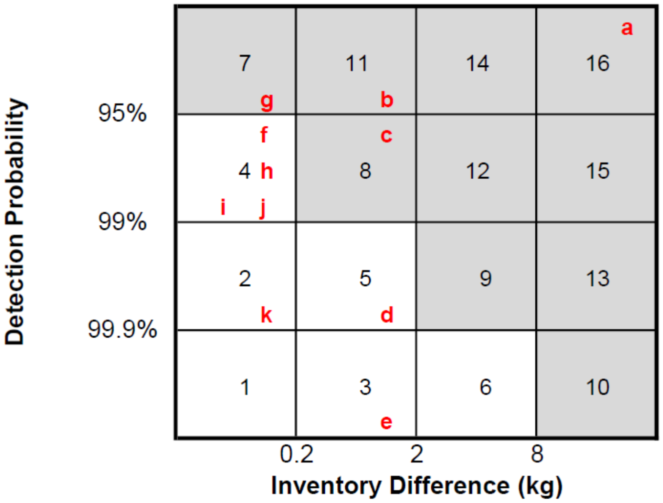


Figure 7. Detection probability versus inventory difference

Table 3. Case legend for Figure 7 and Figure 8

Case	Strategy	σ SNF	σ TRU prod	σ U prod	σ NB	σ Clad	σ Inv
a	Level 1	1%	1%	1%	1%	1%	-
b	Level 2	5%	5%	10%	10%	10%	0.5%
c	Level 2	2%	2%	10%	10%	10%	1%
d	Level 2	1%	1%	1%	1%	1%	1%
e	Level 2	0.5%	0.5%	0.5%	0.5%	0.5%	0.5%
f	Level 3	2%	2%	10%	10%	10%	1%
g	Level 3	1%	3%	10%	10%	10%	1%
h	Level 3	1%	2%	10%	10%	10%	1%
i	Level 4	2%	0.5%	10%	10%	10%	0.5%
j	Level 4	2%	1%	10%	10%	10%	0.5%
k	Level 4	1%	1%	1%	1%	1%	1%

Generally, as measurement uncertainty is decreased within a strategy, the point moves down the matrix (e.g., b to e), and as each additional strategy decreases the ID, the point moves to the left (e.g., d to k).

Upon inspection of the standard deviation in the average ID calculation, it is observed that while SEID is a measure of the detection system, it is not a measure of the variation in ID over several 30-day balance periods. The standard deviation in the average ID calculation for each level is shown in Table 4.

Table 4. PSPM standard deviation average for each strategy

Strategy	ID (kg)	STD
Level 1	85.39	40.04
Level 2	1.8	9.42
Level 3	0.183	0.85
Level 4	0.175	0.75

From Table 4, it is seen that level 1 produces an unsatisfactory strategy — an unacceptable amount of SNM is unaccounted for due to large changes in inventory within the MBA between balance periods. For level 2, even though its ID average was 1.8 kg (meeting acceptance criteria), the standard deviation varied substantially throughout the simulation, while levels 3 and 4 did not have as substantial variations. A positive conclusion that no diversion occurred can be made confidently for levels 3 and 4, although the same cannot be made for level 2. To remedy this observation, a quality factor, QF, is proposed as an empirically derived factor to be applied to the calculated ID.

$$QF = \frac{3 * STD\ of\ \ ID}{SQ\ of\ material} \tag{5}$$

The QF could be determined from operational data or simulated with the PSPM in the absence of operational data. A compensated ID, ID_c, can now be calculated as:

$$ID_c = QF * ID \tag{6}$$

This effectively rewards strategies for low variation in measurements while disadvantaging those with largely varying IDs. Figure 8 reflects the inclusion of the QF with the results shown in Figure 7. Table 4 provides a description of each case. As seen in Figure 8, cases b through e are shifted right an entire risk bin, whereas cases f through k shift to the left to be closer to the center of the bin; point d crosses from acceptable to unacceptable.

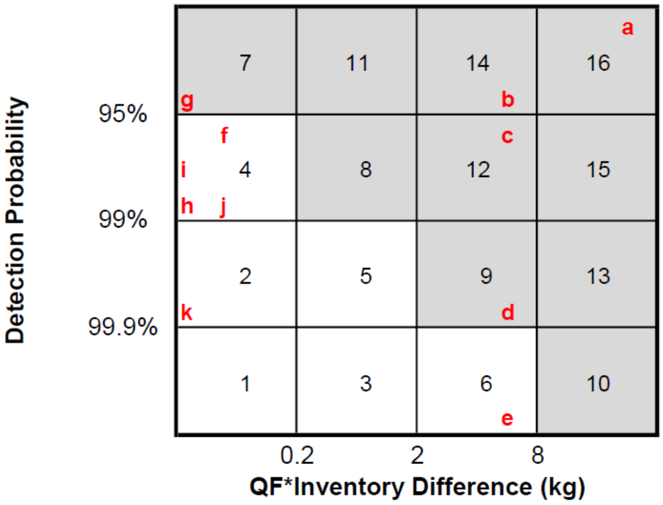


Figure 8. Detection probability versus ID risk matrix

Some important observations from Figure 8 are (1) the conventional safeguards approach is likely unworkable for the reference facility unless detection is capable of uncertainty levels <1% (closer to 0.5% will be needed), and (2) process knowledge is of great benefit to obtaining a material balance closer to zero and allows for possible scenarios with reasonably achievable measurement uncertainties today.

The sensitivity of each measurement contributing to the ID calculation can be demonstrated as well using the PSPM. The SEID calculated for each case (b–k) is shown in Table 5, with each safeguards strategy highlighted as follows: level 2, yellow; level 3, green; and level 4, blue.

Table 5. Top three most sensitive parameters and SEID

Cases	σ SNF	σ TRU prod	σ Inv	σ Clad	SEID (kg)
b	5%	5%	0.5%	10%	5.7089
c	2%	2%	1%	10%	2.3899
d	1%	1%	1%	1%	1.3415
e	0.5%	0.5%	0.5%	0.5%	0.6708
f	2%	2%	1%	10%	2.3949
g	1%	3%	1%	10%	2.5186
h	1%	2%	1%	10%	1.8771
i	2%	0.5%	0.5%	10%	1.7912
j	2%	1%	0.5%	10%	1.9062
k	1%	1%	1%	1%	1.3505

From Table 5, both the input spent fuel measurement and the TRU product measurements greatly dominate the SEID, whereas the other measurements do not have as great an effect. The detection probability will be less than 95% for an ID if s_{SNF} or s_{TRU} are greater than 2%. The cladding measure is less sensitive in the Pu balance because it has such a low Pu concentration (total of ~85 g per balance period), whereas ~85 kg of SNF and TRU product enter/exit the MBA within a 30-day period. Any observed difference represents the amount of Pu inventory within processing vessels or storage at the end of a balance period. Mass tolerances of <1% for a 0–120 kg electronic balance have been documented at FCF.[15] New balances will need to be constructed with mass upper bounds of 1 metric ton, capable of withstanding the high radiation environment in-cell.

The TRU product can be assayed destructively within the cell by drilling a sample from the ingot, or when the ingot is formed, a break off mold is also filled with the same homogenous molten TRU product. The sample can then be analyzed at an analytical lab located onsite using isotopic dilution mass spectroscopy (IDMS), which in a hot cell environment has a total s of 0.28% to 0.42%.[16] Current NDA waste assay techniques can be applied to the cladding waste to achieve a 10% uncertainty.

The most challenging measurement is the SNF fuel. Currently, NDA techniques determine Pu mass to ~10%, although the Next Generation Safeguards Initiative — Spent Fuel (NGSI-SF) project is aiming for ~1%.[17] If only 3% is obtained, very low (~0.5%) mass balance, and TRU product measurements (<0.5%), then this system, case i, could be possible only using a process-informed safeguard strategy. The SHM shows cases e, f, and h through k are acceptable safeguard strategies, with f, h, i, and j most reasonably achievable within the foreseeable future. Cases e and k are not thought to be feasible — SNF uncertainty measurements of <1% — without a breakthrough in the fundamental underlying physics of detection.

Conclusion

To aid in testing proposed safeguards strategies, the Pyroprocessing Safeguards Performance Model and SHM were developed. The PSPM was used to test four strategies: the black box, conventional, process informed, and process informed with rejection sampling, with various measurement uncertainties. These cases were then evaluated with the SHM to assess each case's risk of diversion. An empirically derived QF was developed to provide a measure of the spread of the calculated ID over the course of operation. This assigned less risk to ID measurements with narrow varying measurements while assigning more risk to those with larger variations. Six possible detection scenarios were shown to be of acceptable risk, of which four are achievable within the next 5 years; all use process-informed strategies. It has been shown that including process information, specifically mass balance data from a mass tracking system, significantly reduces the safeguards risk in a pyroprocessing facility.

Acknowledgments

This work is dedicated to the memory of Michael J. Lineberry, who unexpectedly passed away during the development of this work. Michael was a passionate pyroprocessing advocate and a devoted mentor and friend.

References

1. Till, C.E. and Chang, Y.I. 2011. *Plentiful Energy.*
2. Chang, H. et al. 2011. Evaluation of Sigma-MUF (Material Unaccounted For) for the Conceptually Designed Korea Advanced Pyroprocess Facility. *Journal of Korean Physical Society*, *59*(2), 1418–1421.
3. IAEA. 2002. IAEA Safeguards Glossary 2001 edition. Vienna.
4. Burr, T.H. 2013. Revisiting Statistical Aspects of Nuclear Material Accounting. *Science and Technology of Nuclear Installations*.
5. Lineberry, M.E. 2011. Safeguarding the Fast Reactor Fuel Cycle. *Proceedings of the 52th Annual Conference of the Institute of Nuclear Material Management (INMM).*
6. Williamson, M. and Willit, J. 2011. Pyroprocessing Flowsheets for Recycling Used Nuclear Fuel, *Nuclear Engineering and Technology, 43*(4), 329–333.
7. Riley, T. 2014. *Process Informed Safeguards Approach for a Pyroprocessing Facility.* Idaho State University PhD dissertation.
8. Laplace, A.W. 2008. Electrodeposition of Uranium and Transuranics Metals on Solid Cathode. *Nuclear Technology*, 366–372.
9. Riley, T.R., Pope, C.L., and Benedict, R.W. 2016. Safeguards Performance Model for Evaluation of Potential Safeguards Applied to Pyroprocessing Facilities. *Nuclear Engineering and Design, 301*, 157–163.
10. The Mathworks Inc. 2014. MATLAB and Simulink R2014a, Natick, MA

11. Johnson S., Abedin-Zadeh, R., and Pearsall, C. 1997. Development of the Safeguards Approach for the Rokkasho Reprocessing Plant. *IAEA Symposium on Internation Safeguards*. Vienna.
12. Johnson, S.M. 2010. *Designing and Operating for Safeguards: Lessons Learned From the Rokkasho Reprocessing Plant.* PNNL-19626.
13. Pope, C. 2007. *Fast Reactor Spent Fuel Processing: Experience and Criticality Safety.* Idaho National Laboratory.
14. Department of Energy. 2011. Nuclear Material Control and Accountablilty. DOE O 474.2 Chg 1.
15. Orechwa, Y.B. 1997. Startup Calibration and Measurement Control of the Fuel Conditioning Facility In-Cell Electronic Mass Balances. *Journal of Nuclear Materials Management*.
16. IAEA. Nov. 2010. *International Target Value 2010 for Measurement Uncertainities in Safeguarding Nuclear Material.* Vienna.
17. Tobin, S.E. 2013. Update on the Next Generation Safeguards Initiative Spent Fuel Nondestructive Assay Project. *Proceeding of the 54th Annual Meeting of the Institute of Nuclear Materials Management (INMM).*

Identification of Mixed Sources with an Organic Scintillator-Based Radiation Portal Monitor

M. Paff and A. Di Fulvio
Department of Nuclear Engineering and Radiological Sciences, University of Michigan

Y. Altmann
School of Engineering & Physical Sciences, Institute of Sensors, Signals & Systems, Heriot Watt University

S. D. Clarke
Department of Nuclear Engineering and Radiological Sciences, University of Michigan

A. Hero
Department of Electrical Engineering and Computer Sciences, University of Michigan

S. A. Pozzi
Department of Nuclear Engineering and Radiological Sciences, University of Michigan

Abstract

We have developed radionuclide identification algorithms for radiation portal monitor applications. One algorithm uses a spectral angle mapper to match the power spectral density of modified cumulative distribution functions of measured pulse height distributions to reference spectra, whereas the other relies on the decomposition of the observed spectrum as a linear mixture of known radionuclide spectra. Three algorithms were then tested for their ability to perform on-the-fly radionuclide identification on datasets acquired with a liquid organic scintillator-based pedestrian radiation portal monitor on moving special nuclear material and industrial radiological sources, as well as common medical isotopes. We quantified and compared the relative efficacies of the algorithms considered using F-score analysis. Measured radiation sources included 51 g of highly enriched uranium; 6.6 g of weapons-grade plutonium; ^{241}Am, ^{133}Ba, ^{57}Co, and ^{137}Cs sources with activities of several hundred kBq, as well as 260 kBq liquid solution samples of the medical isotopes ^{99m}Tc, ^{111}In, ^{67}Ga, ^{123}I, ^{131}I, and ^{201}Tl. We achieved 100% positive identification for 3-second measurements of single sources moving at a source-transit speed of 1.2 m/s. For mixed sources, with the strongest and weakest sources having no more than a 3:1 ratio of detected counts, encouraging positive identification results were achieved with the unmixing algorithms. Current radiation portal monitor designs suffer from a high incidence rate of nuisance radiation alarms caused in radiation portal monitors by recent nuclear medicine patients and cargo containing large amounts of naturally occurring radioactive materials. Integrating reliable on-the-fly radionuclide identification into the radiation portal monitors could lower the number of nuisance alarms, requiring time-consuming secondary inspections.

Introduction

Thwarting the potential smuggling of nuclear and radiological material across national borders poses many technical challenges. Radiation portal monitors (RPMs) have been extensively deployed in the United States at border crossings for screening incoming vehicles and at major seaports for screening incoming cargo containers. RPMs commonly contain neutron detectors (^{3}He) and gamma detectors (plastic scintillator panels) and look for elevated radiation count rates relative to background when a vehicle or cargo container passes the RPM. The signal from threat materials, like special nuclear material (SNM), might be very weak, especially if SNM is well shielded. Complicating the matter is the fact that measurement times for RPMs are limited to approximately 3 seconds in order to not overly burden the flow of commerce and people.

Actual reported incidents of interdictions of nuclear and radiological materials at border crossings hover around a few dozen events annually worldwide.[1] Yet RPM radiation alarm incident rates of one in hundreds of vehicles or cargo containers are not unheard of. This high alarm rate is due to the prevalence of naturally occurring radioactive material (NORM) in cargo, as well as an increase in nuclear medicine patients over the past decades. Large quantities of NORM-bearing cargo, such as a cargo container filled with kitty litter, and recent nuclear medicine patients — mostly patients who have had ^{99m}Tc procedure within the last few days — emit sufficient gamma radiation to trigger RPM alarms.[2–4] Offending vehicles and cargo containers must be searched with handheld spectroscopic radiation detectors to locate and identify all sources of radiation and ensure that none of them poses a threat to national security. Processing these nuisance alarms can be time-consuming and can distract from the mission of catching smugglers of nuclear and radiological materials.[5]

We are developing an RPM capable of on-the-fly radionuclide identification.[6–9] Such an RPM could distinguish threat from nuisance radiation sources, thus greatly reducing the number of vehicles and cargo containers requiring secondary inspections. Originally, the identification algorithms were developed for identifying single sources of gamma radiation. In reality, many scenarios will involve mixed sources of radiation. Examples include mixed NORM sources, and SNM masked by a NORM source. Two approaches were integrated with our radionuclide identification algorithm to test their ability to handle mixed sources: a linear spectral unmixing algorithm relying on the data only (based on maximum likelihood estimation), and Bayesian approaches that allow the consideration of additional prior knowledge (and based on maximum a posteriori or posterior mean estimation).

Organic Liquid Scintillation Detector-Based Radiation Portal Monitor

We developed and tested a pedestrian radiation portal monitor consisting of eight 7.6 cm diameter by 7.6 cm height cylindrical active volume Eljen EJ309 organic liquid scintillation detectors.[6,8,10] These detectors are sensitive to both neutrons and gammas. Neutron and gamma interactions in the detectors are distinguishable through pulse shape discrimination. The RPM system is scalable to more challenging applications, such as a vehicle RPM.[9,11,12]

Extensive testing occurred at the European Commission Joint Research Centre in Ispra, Italy. The RPM testing facility consists of an electric rail cart system capable of moving radiation sources at speeds up to 3 m/s past the RPMs. Sources tested included 51 g of highly enriched uranium; 6.6 g of weapons-grade plutonium; ^{241}Am, ^{133}Ba, ^{57}Co, and ^{137}Cs sources with activities of several hundred kBq; and various ^{252}Cf spontaneous fission neutron sources.[6,8] In addition, 260 kBq liquid solution samples of the medical isotopes ^{99m}Tc, ^{111}In, ^{67}Ga, ^{123}I, ^{131}I, and ^{201}Tl were measured at the University of Michigan C.S. Mott Children's Hospital. We tested the radionuclide identification algorithms on the measured datasets and their combinations.

On-The-Fly Radionuclide Identification

The on-the-fly radionuclide identification algorithms underwent numerous iterations.[6] Based on F-score analysis,[13] the best identification performance was achieved with an algorithm using a spectral angular mapper[14,15] to compare short measurement time RPM data with library spectra using the power spectral densities of cumulative distribution functions (CDFs) of measured pulsed height distributions (PHDs).[6,7]

To build the library, long measurement time PHDs were obtained for all isotopes of interest. The CDFs, , are formed through integration by computing the probability that takes a value less than — that is, . The quantity is subsequently used. Figure 1 shows for all library spectra as well as for a 3-second measurement of a moving ^{137}Cs source. To characterize the behavior of over its entire energy domain, the following Fourier analysis is used:

$$DFT(k) = \sum_{n=1}^{N} y(n) \exp\left(-i * 2 * pi * (k-1) * \frac{n-1}{N}\right),\ 1 <= k <= N, \qquad (1)$$

where *DFT(k)* is the amount of frequency in the signal, *y(n)* is the modified CDF, *n* is the sample energy domain, *N* is the number of samples, and *k* is the sample in the frequency domain.

For a CDF signal, the power spectral density (Equation 2) computes how "power" is distributed over frequency of the CDF by computing the squared modulus of the DFT:

$$PSD(k) = |DFT(k)|^2. \qquad (2)$$

Finally, the spectral angle is computed between the power spectral density of the short measurement time RPM data and all of the power spectral densities of the library spectra. The smallest then represents the best fit

$$\alpha_i = \cos^{-1}\left[\frac{(PSD(k) \cdot PSD_{matrix}(:,i))}{\|PSD(k)\|\|PSD_{matrix}(:,i)\|}\right],[14]. \qquad (3)$$

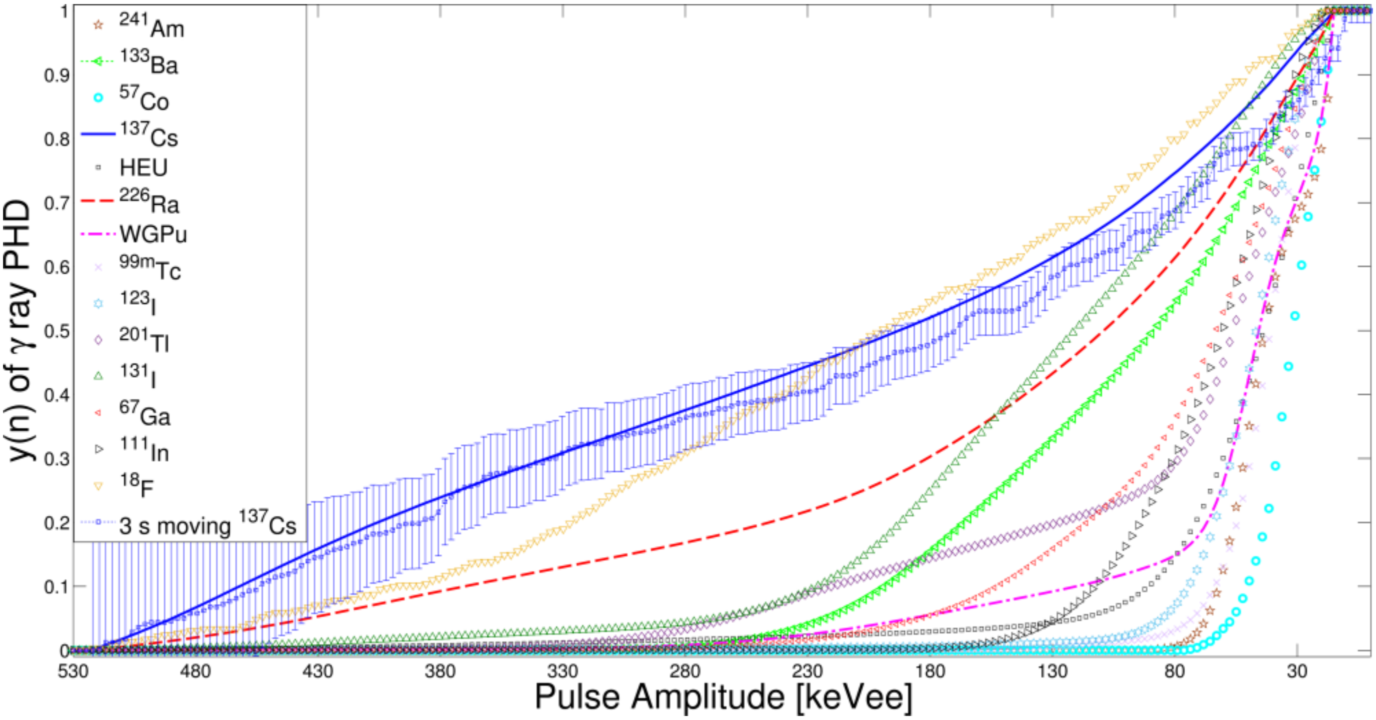


Figure 1. Modified CDF library matrix with of moving ^{137}Cs source acquired with pedestrian RPM at the second SCINTILLA benchmark at the Joint Research Centre in Ispra, Italy, in February 2014[6]

Identification of Mixed Gamma Sources

Mixed sources — that is, scenarios in which the signatures of multiple radionuclides are present —are of great concern to designers of spectroscopic RPMs. In particular, the masked source scenario, in which a strong NORM source masks the weaker SNM source, poses a challenge to identification algorithms. In traditional gamma spectroscopy with inorganic scintillators — for example, NaI(Tl) — mixed sources pose no significant challenge as long as the detector energy resolution suffices to resolve all present photopeaks. For organic scintillator-based RPMs, however, photopeaks do not exist, and the entire PHD forms the signal, so a mixed source RPM response will be a linear combination of individual source responses.

It is important that any unmixing algorithm does not misidentify a mixed source RPM response as some other single source. Conversely, the algorithm must identify all constituent components in the mixed source and also estimate the relative activities of the constituent sources.

Linear Spectral Unmixing Approach

Linear spectral unmixing (LSU) algorithms can be used to decompose a mixed signal into its constituent components.[16–18] A mixed signal consists of a linear combination of possible radionuclides at different fractions:

$$M \approx c_1S_1 + c_2S_2 + \cdots + c_nS_n. \tag{4}$$

Solving for the mixing coefficients such that the sum on the right side of Equation 4 approximates , while accounting for the physical constraints to (Equation 5), provides the relative activities of library spectra present in the mixed source response:

$$\min_{c\geq 0}\|\boldsymbol{S} * c - M\| \ . \tag{5}$$

The unmixing algorithm can be tested on various forms of the RPM data, such as PHDs, CDFs, or power spectral densities of the CDFs. Different mixed source scenarios were tested by mixing together measured PHDs from individual sources in different ratios. Figure 2 shows the LSU results for six different tested mixtures. For each mixture, 30 mixed PHDs of this composition were

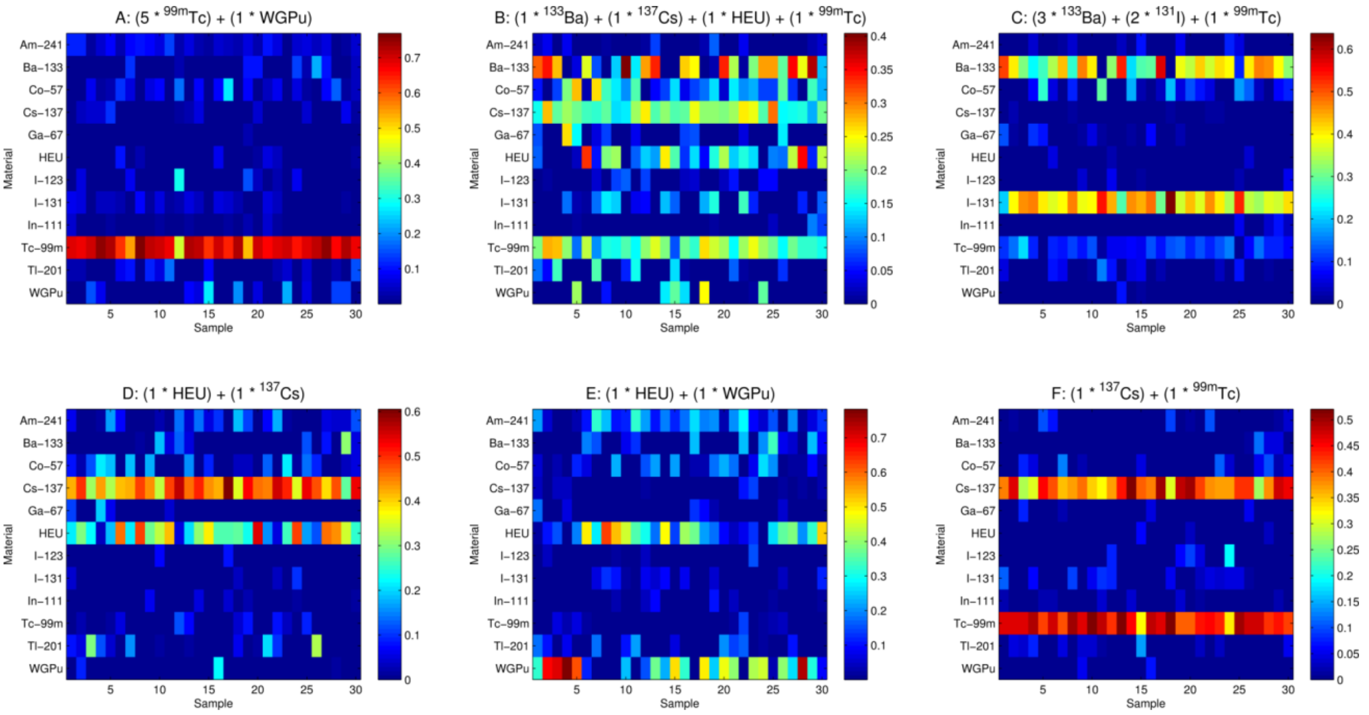


Figure 2. LSU computed coefficients computed for 30 samples of each of six different mixtures created from RPM-measured gamma-radiation data

created and unmixed with the LSU algorithm, as illustrated by the 30 samples shown for each mixture in Figure 2. The average coefficients computed for all library radionuclides are shown as color bars. The only constraint applied is that all coefficients have to be non-negative.

Bayesian Estimators

As an alternative to the LSU technique presented above, which implicitly relies on an additive white Gaussian noise assumption, we also use Bayesian estimators on a Poisson noise model where *M* is our observed data — that is, some RPM-measured response to a mixed source of gamma radiation — and *x* is our unknown mixing contribution of different sources in our gamma library. This results in the prior distribution: *f*(c), which enforces c>0.

Following Bayes' rule, the posterior distribution of *c* given *M* therefore is *f*(c|M). To solve for the mixing contribution coefficients *c*, we can maximize *f*(c|M) — maximum a posteriori (MAP) estimation — which provides us with the a posteriori most likely solution. The coefficients *c* are then calculated as the mode of the posterior distribution. A different approach consists of computing the expectation of c|M — that is, the posterior mean — which will minimize the mean square error between the estimated and observed data. This technique is known as minimum mean squared error (MMSE) estimation. The MAP results for the same mixtures used for the LSU in Figure 2 are shown in Figure 3, and the MMSE results are shown in Figure 4. Once again, the only constraint is that all coefficients are non-negative.

Similar to the LSU method, both the MAP and MMSE methods struggle when more than two sources are present (mixture B) or when a weaker source is masked by a stronger source (mixture A).

Under these conditions, up to 12 sources could be present. This might not be realistic for real-world RPM measurements, so the Bayesian estimator should improve if we promote the sparsity of the mixture by fixing for instance the maximum number of sources in the solution. For the MAP results shown in Figures 5, 6, and 7, the maximum number of sources in any possible solution are constrained to two, three, or four sources, respectively. As expected, the results improve dramatically if the solution is constrained to the correct number of solutions. The results do not degrade significantly if the constrained number of solutions does not greatly exceed the actual number of sources present in the mixture either.

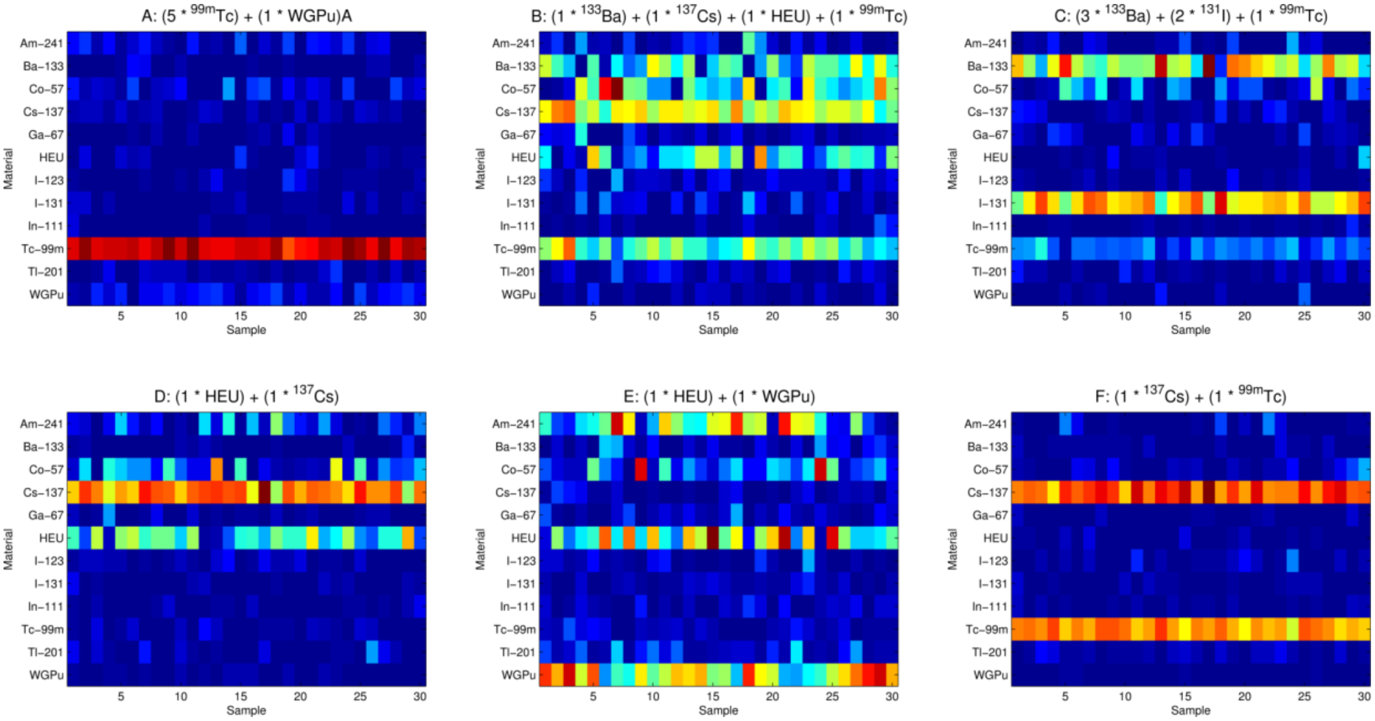


Figure 3. MAP computed coefficients computed for 30 samples of each of six different mixtures created from RPM-measured gamma-radiation data

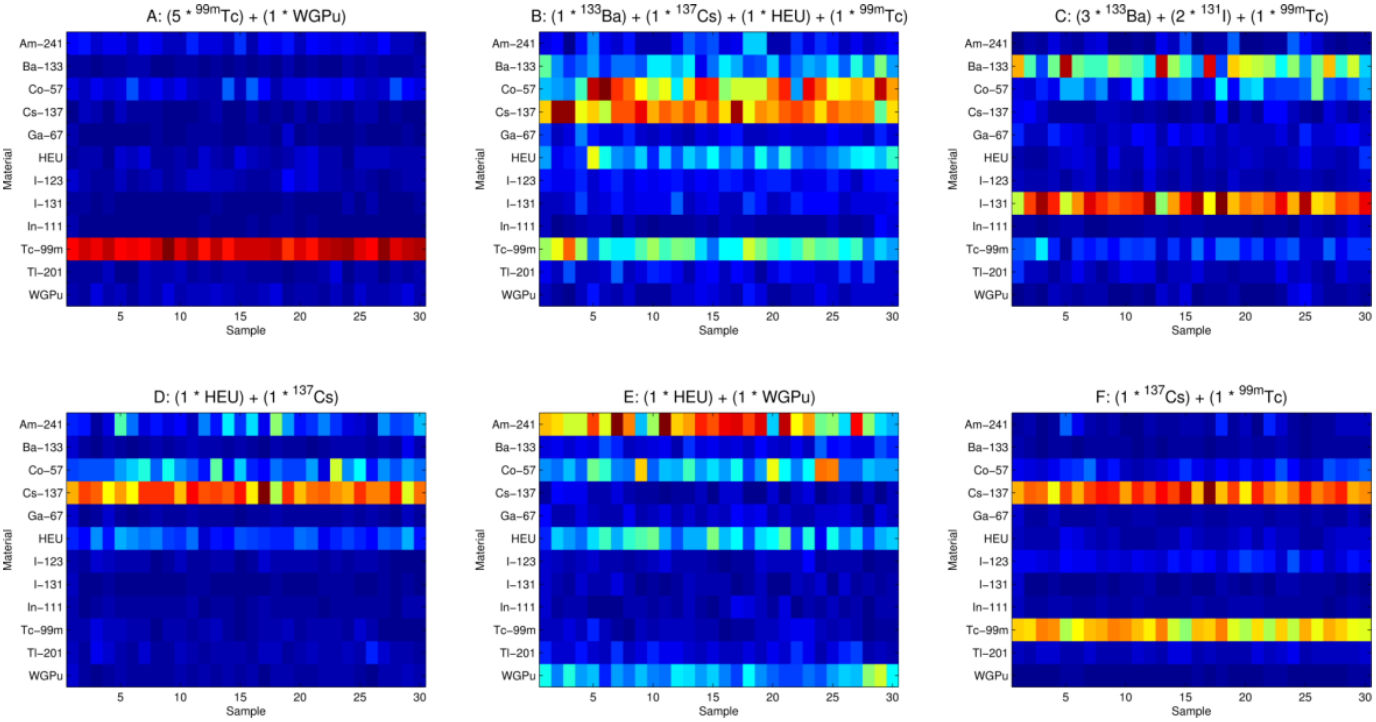


Figure 4. MMSE computed coefficients computed for 30 samples of each of six different mixtures created from RPM-measured gamma-radiation data

Figure 8 shows the correlation matrix for one sample of mixture B (^{137}Cs + HEU + ^{99m}Tc + ^{133}Ba). The correlation matrix shows that the Bayesian estimator (that is, the MAP estimator) struggles to distinguish ^{99m}Tc from ^{123}I as well as ^{133}Ba from ^{131}I. In other words, the estimator knows with high confidence that, for example, either ^{99m}Tc or ^{123}I is present in the mixture, but it can't necessarily say which of the two is present. Looking at Figure 1, we see that ^{99m}Tc and ^{123}I exhibit very similar CDFs, thus explaining why the Bayesian estimator struggles to discern these sources. Such correlation matrices provide an additional tool when SNM might be mistakenly misidentified as some less-threatening radionuclide with a similar RPM-measured response.

The different unmixing methods can be compared via the mean squared error for the different possible composition solutions. Tables 1 and 2 show the average compositions of 30 samples of mixed sources E (HEU and WGPu mixed 1:1) and B (^{137}Cs + HEU + ^{99m}Tc + ^{133}Ba mixed in equal proportions) as computed with the MAP Bayesian estimator, with the number of allowed constituent sources in the solution constrained to various value. Tables 1 and 2 also include compositions computed with the MMSE Bayesian estimator and with the LSU method.

The MAP estimator most accurately estimates the composition of the mixed sources, assuming that the solution is not constrained to fewer sources than are actually present. Constraining the MAP estimator to some value greater than the number of present sources (for example, > 2 for mixture E) but well below the 12 total number of sources in the library does not lead to significant degradation of the composition estimates (see MAP with five sources for mixture E). On average, the unconstrained MAP, MMSE, and LSU techniques for the most part estimate the correct sources present in the mixtures, but relative to the constrained MAP solutions, these other techniques exhibit less consistency and show poorer performance for estimating the relative abundancies of sources present in the mixtures.

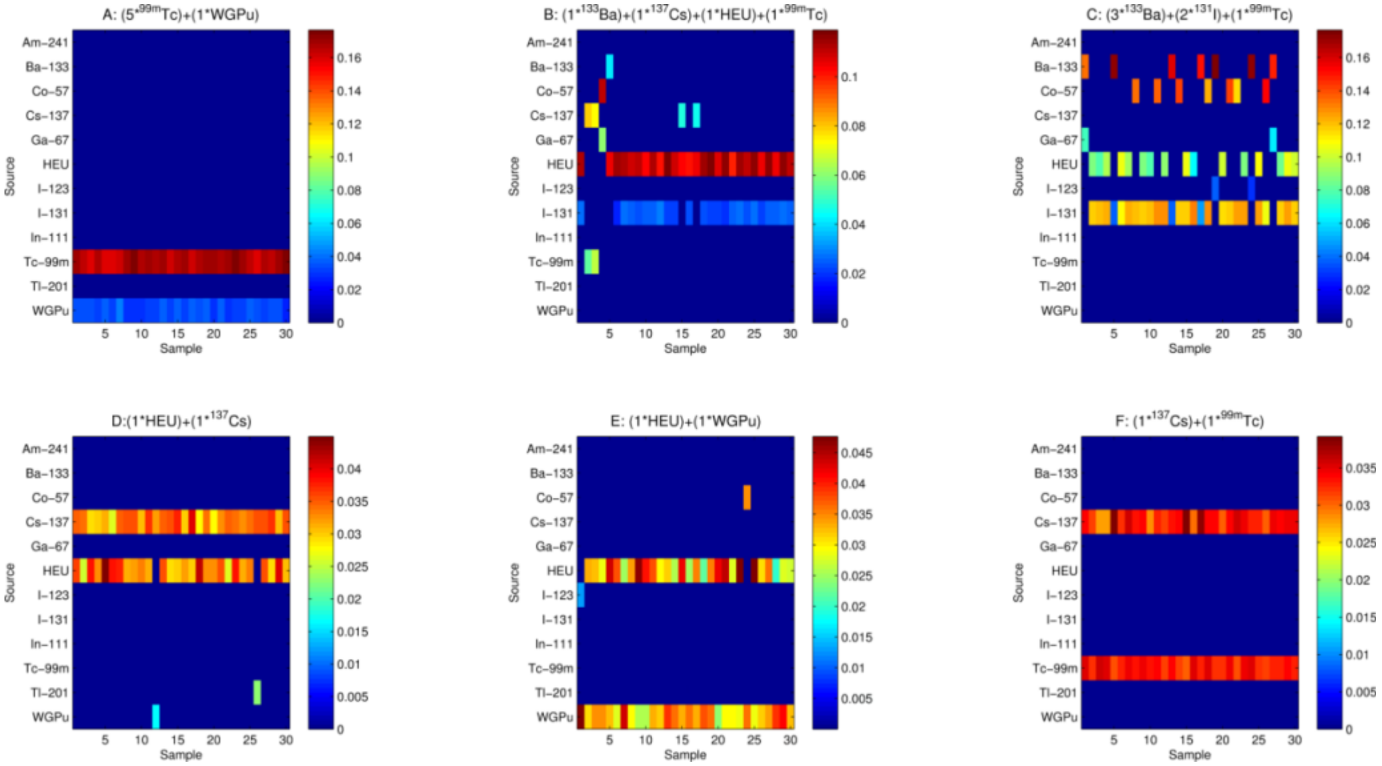


Figure 5. MAP computed coefficients computed for 30 samples of each of six different mixtures created from RPM-measured gamma-radiation data, with the number of solutions constrained to two

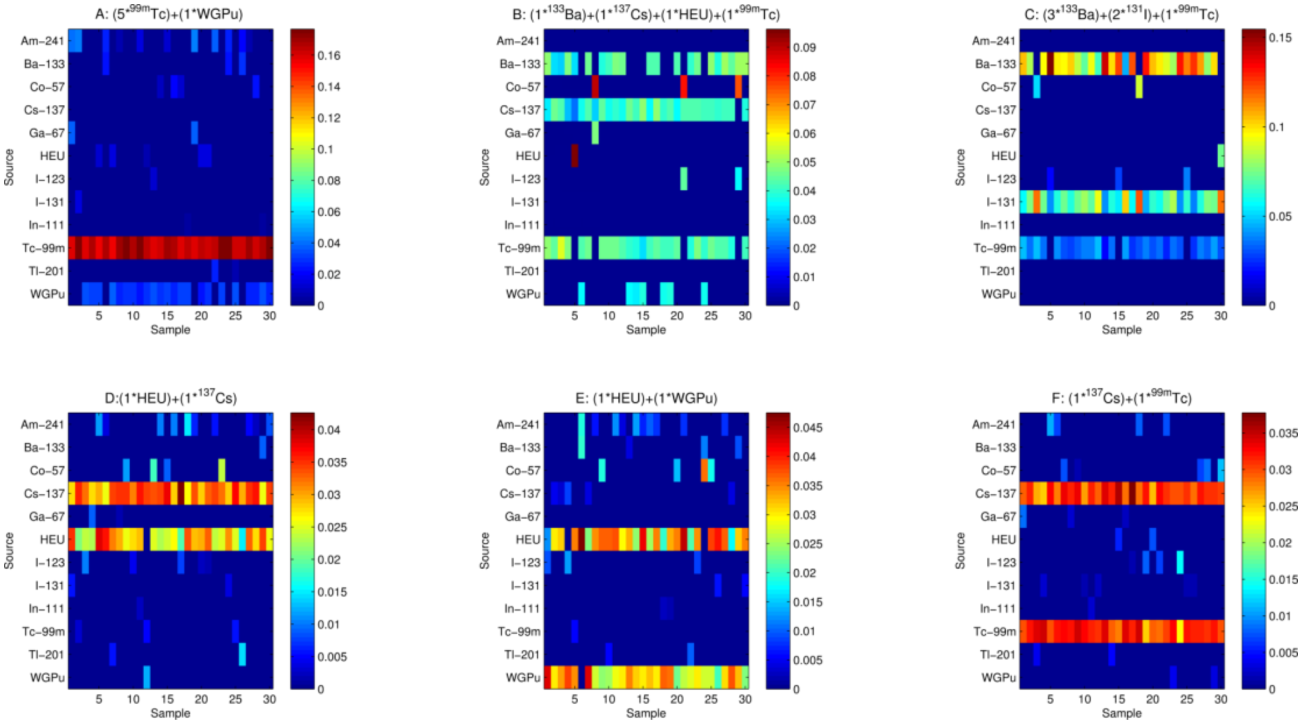


Figure 6. MAP computed coefficients computed for 30 samples of each of six different mixtures created from RPM-measured gamma-radiation data, with the number of solutions constrained to three

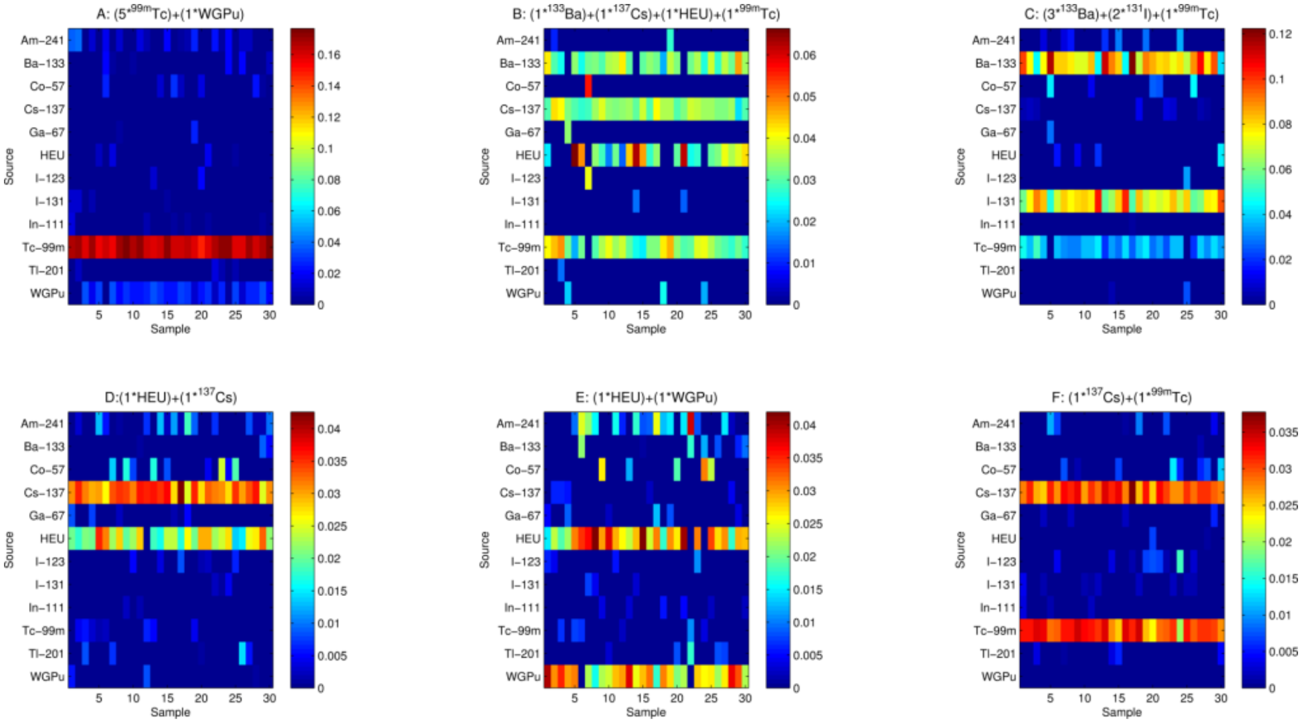


Figure 7. MAP computed coefficients computed for 30 samples of each of six different mixtures created from RPM-measured gamma-radiation data, with the number of solutions constrained to four

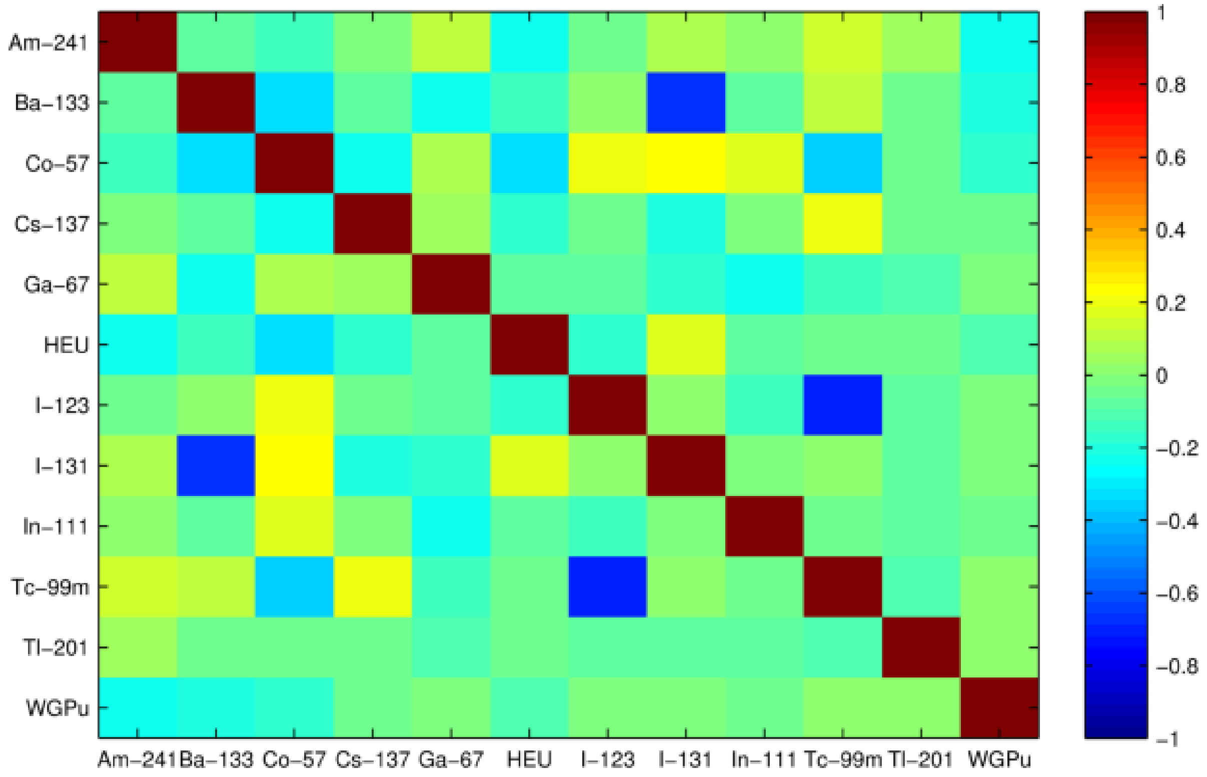
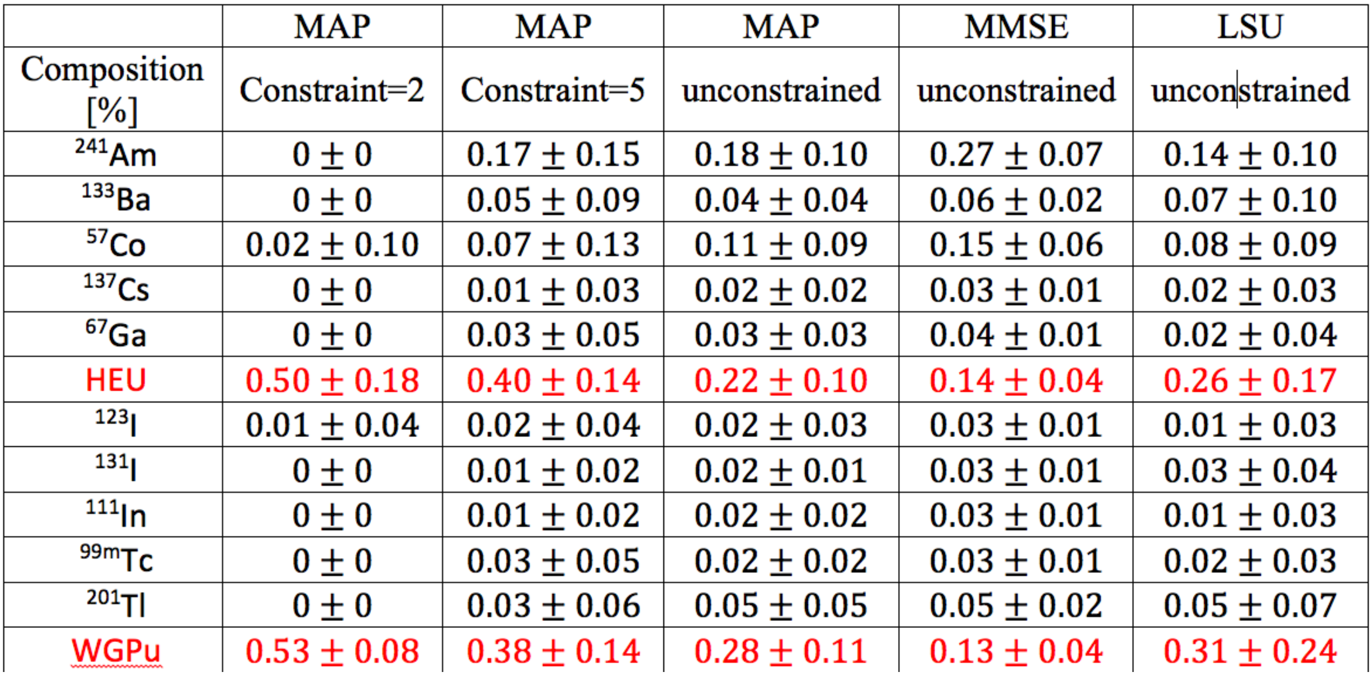


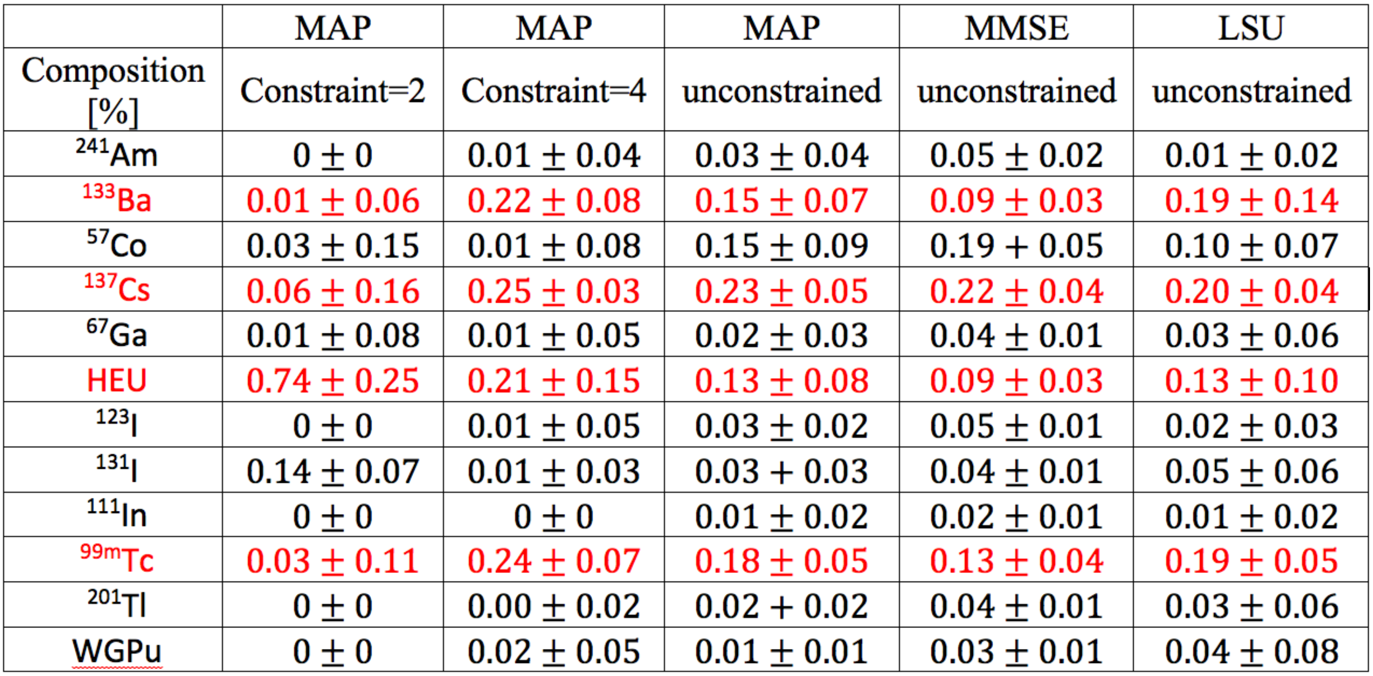
Figure 8. Correlation matrix for mixture B (^{137}Cs + HEU + ^{99m}Tc + ^{133}Ba) showing that the Bayesian estimator struggles to distinguish ^{99m}Tc from ^{123}I as well as ^{133}Ba from ^{131}I

Table 1. Mean squared error for computed coefficients for 30 samples of mixture E (HEU and WGPu mixed 1:1) for different unmixing algorithms. For MAP, the number of possible solutions is constrained to two, five, or all possible sources.



	MAP	MAP	MAP	MMSE	LSU
Composition [%]	Constraint=2	Constraint=5	unconstrained	unconstrained	unconstrained
^{241}Am	0 ± 0	0.17 ± 0.15	0.18 ± 0.10	0.27 ± 0.07	0.14 ± 0.10
^{133}Ba	0 ± 0	0.05 ± 0.09	0.04 ± 0.04	0.06 ± 0.02	0.07 ± 0.10
^{57}Co	0.02 ± 0.10	0.07 ± 0.13	0.11 ± 0.09	0.15 ± 0.06	0.08 ± 0.09
^{137}Cs	0 ± 0	0.01 ± 0.03	0.02 ± 0.02	0.03 ± 0.01	0.02 ± 0.03
^{67}Ga	0 ± 0	0.03 ± 0.05	0.03 ± 0.03	0.04 ± 0.01	0.02 ± 0.04
HEU	0.50 ± 0.18	0.40 ± 0.14	0.22 ± 0.10	0.14 ± 0.04	0.26 ± 0.17
^{123}I	0.01 ± 0.04	0.02 ± 0.04	0.02 ± 0.03	0.03 ± 0.01	0.01 ± 0.03
^{131}I	0 ± 0	0.01 ± 0.02	0.02 ± 0.01	0.03 ± 0.01	0.03 ± 0.04
^{111}In	0 ± 0	0.01 ± 0.02	0.02 ± 0.02	0.03 ± 0.01	0.01 ± 0.03
^{99m}Tc	0 ± 0	0.03 ± 0.05	0.02 ± 0.02	0.03 ± 0.01	0.02 ± 0.03
^{201}Tl	0 ± 0	0.03 ± 0.06	0.05 ± 0.05	0.05 ± 0.02	0.05 ± 0.07
WGPu	0.53 ± 0.08	0.38 ± 0.14	0.28 ± 0.11	0.13 ± 0.04	0.31 ± 0.24

Table 2. Mean squared error for computed coefficients for 30 samples of mixture B (^{137}Cs + HEU + ^{99m}Tc + ^{133}Ba mixed in equal proportions) for different unmixing algorithms. For MAP, the number of possible solutions is constrained to two, four, or all possible sources.



	MAP	MAP	MAP	MMSE	LSU
Composition [%]	Constraint=2	Constraint=4	unconstrained	unconstrained	unconstrained
^{241}Am	0 ± 0	0.01 ± 0.04	0.03 ± 0.04	0.05 ± 0.02	0.01 ± 0.02
^{133}Ba	0.01 ± 0.06	0.22 ± 0.08	0.15 ± 0.07	0.09 ± 0.03	0.19 ± 0.14
^{57}Co	0.03 ± 0.15	0.01 ± 0.08	0.15 ± 0.09	0.19 + 0.05	0.10 ± 0.07
^{137}Cs	0.06 ± 0.16	0.25 ± 0.03	0.23 ± 0.05	0.22 ± 0.04	0.20 ± 0.04
^{67}Ga	0.01 ± 0.08	0.01 ± 0.05	0.02 ± 0.03	0.04 ± 0.01	0.03 ± 0.06
HEU	0.74 ± 0.25	0.21 ± 0.15	0.13 ± 0.08	0.09 ± 0.03	0.13 ± 0.10
^{123}I	0 ± 0	0.01 ± 0.05	0.03 ± 0.02	0.05 ± 0.01	0.02 ± 0.03
^{131}I	0.14 ± 0.07	0.01 ± 0.03	0.03 + 0.03	0.04 ± 0.01	0.05 ± 0.06
^{111}In	0 ± 0	0 ± 0	0.01 ± 0.02	0.02 ± 0.01	0.01 ± 0.02
^{99m}Tc	0.03 ± 0.11	0.24 ± 0.07	0.18 ± 0.05	0.13 ± 0.04	0.19 ± 0.05
^{201}Tl	0 ± 0	0.00 ± 0.02	0.02 + 0.02	0.04 ± 0.01	0.03 ± 0.06
WGPu	0 ± 0	0.02 ± 0.05	0.01 ± 0.01	0.03 ± 0.01	0.04 ± 0.08

Conclusion

Techniques were developed to process RPM gamma measurements from mixed sources with up to four different radionuclides out of a library of 12 known radionuclides. The LSU and Bayesian MAP and MMSE techniques estimate which sources are present in the RPM mixed gamma response and at what relative compositions. Constraining the MAP estimator to solutions with five or fewer radionuclides produced accurate and consistent results for the six mixtures tested. For each mixture, 30 independent samples were tested with each algorithm.

The ability to decompose mixed sources of radiations is crucial for spectroscopic RPMs. Spectroscopic RPMs must be able to detect weak SNM sources masked by a stronger NORM or nuisance radiation source. RPM on-the-fly radionuclide algorithms must also be able to handle mixed sources of NORM and nuisance sources, such as truckload of kitty litter (^{40}K) with a truck driver with a recent nuclear medicine procedure (^{99m}Tc). Future work will look into more challenging masking scenarios and the expansion of the source library.

Acknowledgments

This work was supported in part by the Consortium for Verification Technology under Department of Energy National Nuclear Security Administration award number DE-NA0002534.

References

1. IAEA. 2015. IAEA Incident and Trafficking Database (ITDB). www-ns.iaea.org/downloads/security/itdb-fact-sheet.pdf.
2. Kouzes, R.T., Ely, J. H., Geelhood, B. D., Hansen, R. R., Lepel, E.A., Schweppe, J.E., Siciliano, E.R., Strom, D.J., and Warner, R.A. 2003. Naturally Occurring Radioactive Materials and Medical Isotopes at Border Crossings. *Nucl. Sci. Symp. Conf. Rec.* 1448–1452, doi:10.1109/NSSMIC.2003.1351967.
3. Kouzes, R.T. and Siciliano, E.R. The Response of Radiation Portal Monitors to Medical Radionuclides at Border Crossings. 2006. *Radiat. Meas. 41*, 499–512, doi:10.1016/j.radmeas.2005.10.005.
4. Geelhood, B.D., Ely, J.H., Hansen, R.R., Kouzes, R.T., Schweppe, J.E., and Warner, R.A. 2004. Overview of Portal Monitoring at Border Crossings. *Nucl. Sci. Symp. Conf. Rec.* 513–517, doi:10.1109/NSSMIC.2003.1352095.
5. PNNL. 2016. Radiation Detectors at U.S. Ports of Entry Now Operate More Effectively, Efficiently, www.pnnl.gov/news/release.aspx?id=4245.
6. Paff, M.G. 2017. Organic Scintillation Detectors for Spectroscopic Radiation Portal Monitors. University of Michigan, Ann Arbor, doi:10.13140/RG.2.2.25287.29605.
7. Paff, M.G., Di Fulvio, A., Clarke, S.D., and Pozzi, S.A. 2017. Radionuclide Identification Algorithm for Organic

Scintillator-Based Radiation Portal Monitor. *Nucl. Instruments Methods Phys. Res. Sect. a-Accelerators Spectrometers Detect. Assoc. Equip. 849C*. 41–48, doi:http://dx.doi.org/10.1016/j.nima.2017.01.009.

8. Paff, M.G., Ruch, M.L., Poitrasson-Riviere, A., Sagadevan, A., Clarke, S.D., and Pozzi, S. 2015. Organic Liquid Scintillation Detectors for On-the-Fly Neutron/Gamma Alarming and Radionuclide Identification in a Pedestrian Radiation Portal Monitor. *Nucl. Inst. Methods Phys. Res. A. 789*, 16–27, doi:10.1016/j.nima.2015.03.088.
9. Paff, M.G., Clarke, S.D., and Pozzi, S.A. 2016. Organic Liquid Scintillation Detector Shape and Volume Impact on Radiation Portal Monitors. *Nucl. Instruments Methods Phys. Res. Sect. A Accel. Spectrometers, Detect. Assoc. Equip. 825*, 31–39, doi:10.1016/j.nima.2016.03.102.
10. Paff, M., Ruch, M., Sagadevan, A., Clarke, S.D., Pozzi, S.A., and Peerani, P. 2014. Performance of a EJ309 Organic Liquid Scintillation Detector Pedestrian Radiation Portal Monitor Prototype at the 2nd SCINTILLA Benchmark Campaign. *Proc. 55th Annu. Meet. Inst. Nucl. Mater. Manag.*
11. Paff, M.G., Clarke, S.D., and Pozzi, S.A. 2016. Optimization of Organic Liquid Scintillation Detectors in Radiation Portal Monitor Applications. *IEEE Symp. Radiat. Meas. Appl.*, Berkeley, CA, USA.
12. Ruch, M., Paff, M., Poitrasson-Riviere, A., Sagadevan, A., Clarke, S.D., Pozzi, S.A., and Peerani, P. 2015. Large Volume Organic Liquid Scintillation Detectors as a Vehicle Radiation Portal Monitor Prototype at the 3rd SCINTILLA Benchmark Campaign. *Proc. 56th Annu. Meet. Inst. Nucl. Mater. Manag.*
13. Sokolova, M. and Lapalme, G. 2009. A Systematic Analysis of Performance Measures for Classification Tasks. *Inf. Process. Manag. 45*, 427–437, doi:10.1016/j.ipm.2009.03.002.
14. Kruse, F.A., Lefkoff, A.B., Boardman, J.W., Heidebrecht, K.B., Shapiro, A.T., Barloon, P.J., and Goetz, A.F.H. 1993. The Spectral Image Processing System (SIPS) Interactive Visualization and Analysis of Imaging Spectrometer Data. *Remote Sens. Environ. 44*, 145–163. doi:10.1016/0034-4257(93)90013-N.
15. Yuhas, R.H., Goetz, A.F.H., and Boardman, J.W. 1992. Discrimination Among Semi-arid Landscape Endmembers Using the Spectral Angle Mapper (SAM) Algorithm. *JPL, Summ. Third Annu. JPL Airborne Geosci. Work. Vol. 1 AVIRIS Work.* 147–149, http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19940012238.pdf.
16. Yang, J. and He, Y. 2017. Automated Mapping of Impervious Surfaces in Urban and Suburban Areas: Linear Spectral Unmixing of High Spatial Resolution Imagery. *Int. J. Appl. Earth Obs. Geoinf. 54*, 53–64, doi:http://dx.doi.org/10.1016/j.jag.2016.09.006.
17. Uhrin, A. V. and Townsend, P.A. 2016. Improved Seagrass Mapping Using Linear Spectral Unmixing of Aerial Photographs. *Estuar. Coast. Shelf Sci. 171*, 11–22, doi:http://dx.doi.org/10.1016/j.ecss.2016.01.021.
18. Rommel, D., Grumpe, A., Patrik, M., Wöhler, C., Mall, U. and Kronz, A. 2017. Automatic Endmember Selection and Nonlinear Spectral Unmixing of Lunar Analog Minerals. *Icarus 284*, 126–149, doi:http://dx.doi.org/10.1016/j.icarus.2016.10.029.

Book Review

Mark L. Maiello, PhD
Book Review Editor

Insider Threats

Edited by Mathew Bunn and Scott Sagan
Softcover, 181 pages
ISBN 978-1-5017-0516-8
Cornell University Press, Ithaca and London, 2016

Can the insider threat experience of non-nuclear industries and incidents inform the insider threat planning of nuclear security operations? The contention of editors Bunn and Sagan is yes. Their effort is to do so is this short treatise written with seven other experts. This interesting take on the subject was motivated — until now — by the lack of information and data on the subject within the nuclear industry. The editors have looked to the casino and pharmaceutical industries and well-known incidents such as the anthrax mailing attacks of 2001, in addition to insider attacks at military bases, to get out ahead of a nuclear insider threat incident.

The editors performed unprecedented research into the problem area. The results indicate that there have been many incidents of insider threats at nuclear facilities, but few linked to terrorists. The paucity of *jihadi* interest — as measured by Internet forum activity and other research — further diminishes the probability of a terrorist threat. Even when terrorists consider a nuclear target, assault rather than infiltration appears to be their choice. From 1970 to 2012, of the 113,000 terrorist events recorded, only 58 involved nuclear targets — and of those, only four involved an insider. Yet Bunn and Sagan pressed on to produce this book, indicating that the threat — if ever carried out — is simply too dangerous to ignore.

Insiders are personnel within government, military, academic, and private-sector facilities with access to potentially dangerous information, procedures, or hazardous materials. They obviously need not be or be affiliated with terrorists. A grudge, an exaggerated sense of unfair treatment, mental imbalance, or other factors may push a disgruntled employee to take actions that endanger colleagues and/or the public. And herein lies another concern: according to the editors, the insider threat is viewed with some complacency by most employers. Pre-employment vetting by background checks is frequently viewed as adequate but is, of course, dependent on the depth of the investigation process. It also fails to take into account the time-dynamics of human nature: people and their circumstances change. They have normal human failings and they sometimes suffer unfortunate changes to their work life and in their relationships. They are subject to illness, aging, personal loss, and grief. Will some cross the line into dangerous behavior if they undergo these misfortunes?

A compelling example of the effort put forward in this book is the story of the anthrax attacks of September 2011, penned by contributors Jessica Stern and Ronald Schouten. The authors summarize the investigation by law enforcement, extensively portray the insider, explain how the red flags the insider exhibited were ignored, and describe the institutional security and law enforcement changes that resulted from the success of the attacks. This is one of the best known and effective insider attacks, and so it is worthy not only of inclusion in the book but of some discussion here.

The investigation began shortly after the September 11, 2001 terrorist attacks in New York City and Washington, D.C. The FBI eventually focused on microbiologist Dr. Bruce Ivins of the U.S. Army Medical Research Institute of Infectious Disease (USAMRIID). Ivins' success — temporarily abetted by the FBI's initial focus on another researcher, Steven Hatfill — was due to a swirl of regulatory changes, business culture, inattention to the dangerous signals he sent, and luck. Perhaps most disturbing, but most relevant to the mission of the book, were two key issues: the rather obvious signals he sent regarding his mental health that were not acted upon, and the circumstance of the background checks that initiated his security clearance and maintained it through several reinvestigations over 28 years.

Ivins, a product of a traumatic childhood, had been under psychiatric care since 1978. In previous years, he had committed burglaries of sorority houses in retaliation for being shunned by sorority sisters in his higher education days. Even at this early stage, his doctor knew of these acts and his more heinous desires to poison a former sorority sister he had become obsessed with. Little or nothing of this early history of aberrant behavior — which, it must be reiterated, included criminal behavior — was made part of his later security assessments. In 1980, his 20-year career with USAMRIID commenced, along with his remarkable story of mental health decline that never was red-flagged by his superiors or the security establishment, despite Ivins' revelations to those around him of his concern for his own mental health.

Ivins had obsessive relationships with female technicians who worked for him, confiding in them about his mental state. Despite some pretty strong and frightening admissions in written emails to these colleagues (he mentioned excessive drinking and a growing paranoia), the concerns were never transmitted to Ivins' superiors. When he hacked into the technicians' emails to determine what they thought of him and found some unflattering messages, he felt so betrayed that he planned to poison of one of them. Running counter-current with this aberrant behavior was his devotion to community service. Ivins was, for example, very active in his church.

His awareness of his mental troubles caused him to seek therapy. Although he had not sought help since 1980, he resumed it after a 20-year hiatus in January 2000. A major factor in his ability to pull off the anthrax attacks was the failure of his doctors to recognize his past history and the depth of his illness and to communicate their concerns to USAMRIID.

Such fragmented and failed communications had a singular effect: they failed to ban Ivins from access to biological select agents and toxins (BSATs) and the biocontainment labs where they were manipulated. (Ivins logged his time in the labs — even his unusual nighttime and weekend hours — but they were not reviewed in timely fashion). Once the FBI investigation began, Ivins did all he could to subvert it. He failed to supply untainted anthrax samples from the lab, and he tried to direct suspicion away from himself to other researchers.

The red flags that permeate Ivins' duplicitous and secretive behavior were missed. This was due to the normalization of his behavior. In short, his colleagues became used to "Ivins being Ivins." He became the harmless eccentric.

USAMRIID investigators never spoke to the clinicians and therapists who treated Ivins. Some of these mental health specialists were extremely concerned about Ivins, diagnosing him as a sociopath and homicidal. Over the years, Ivins did complete mental health and security review forms. Although inconsistent in his entries, the information he did supply was telling but was never followed up on. No one save his private clinicians knew of his mental condition, and they were unaware of his work with BSAT. The crucial connection to dangerous materials was never made. Some of these clinicians later indicated that they would have recommended restricting him from BSATs. Although the background check system (largely forms to fill out) was deemed a sufficient practice to approve clearance to work at USAMRIID, it failed to capture Ivins' use of anti-psychotic medicine.

Organizational bias also was a factor. In addition to Ivins being a familiar face with known eccentricities, leadership was apparently unwilling to change security measures without a proven outcome — that is, the removal of an insider threat. This attitude is an example of "Not in My Organization," the bias that an insider threat simply could not exist at one's place of employment. The end result of all this: Ivins was able to mail anthrax spores to offices of the *New York Times*, the *New York Post*, and the *National Enquirer*. Senate Majority Leader Tom Daschle and Senator Patrick Leahy also received letters. By November 2001, five people were dead and 17 infected. Investigators took nearly 7 years to zero in on Ivins, who became increasingly distressed by the pressure put on him by law enforcement. He committed suicide in July 2008.

As indicated by this summary, contributors Stern and Schouten provide all the necessary background material for the reader to make sense of the insider threat, including the perpetrator's motives and the security failures that enabled the threat to succeed. An equally detailed analysis of these failures and the steps taken to overcome the deficiencies are part of the book's objectives and appear to be sound advice, even if the reader does not immediately see the connection to nuclear facility operations. It does become quite clear later that this is a book about organizational failure to which nuclear facilities of all types are vulnerable.

Other insider threat events that are analyzed in the book include the Fort Hood, Texas, Terrorist Attack of 2009, in which U.S. Army Major Nidal Hasan killed 13 Defense Department employees (by Amy B. Zegart). Another chapter covers the multiple Afghan National Security Force attacks on the International Security Assistance Force from 2001 to roughly 2014 (Austin Long). Another seeks to summarize the lessons learned from the security programs in the pharmaceutical and casino industries (Bunn and Kathryn M. Glynn). A final chapter presents a worst practices guide gleaned from these insider threat reviews (Bunn and Sagan again). Here, they analyze 10 assumptions made by management and security forces that can lead to insider threat success. For example, the reader will find sections on "Assume That Serious Insider Problems Exist Elsewhere Are Not in My Organization (NIMO)," "Assume that Background Checks Will Catch All Insider Threats," and "Assume that Organizational Culture and Employee Disgruntlement Don't Matter." They are not ranked in importance or frequency of occurrence. All matter and apparently contribute equally to the problem.

A book that goes into this much detail about non-nuclear issues had better be a good read for those in nuclear non-proliferation, or else it is likely to be ignored. *Insider Threats* does not disappoint. Aside from the intriguing recounts of the incidents, the writing is clear, concise, and consistently interesting. The few black-and-white illustrations, tables, and figures are concise and useful. The book is supported by a serviceable index of about six pages.

This is a thought-provoking book that goes outside our customary playing field of nuclear non-proliferation. Focused on security and, at that, a narrower problem within the security universe, this book brings a new perspective to the issue of insider threats by utilizing the larger world's experience with this ever-present danger. It is a good example of reaching out beyond traditional boundaries for the purposes of seeking new insights. As such, it quietly achieves its scholarly mission.

Taking the Long View in a Time of Great Uncertainty
New Challenges for the Institute

Jack Jekowski
Industry News Editor and Chair of the Strategic Planning Committee

This year's 59th Annual Meeting, held at the Marriott Waterfront in Baltimore, was a nonstop, action-packed event that incorporated new formats, interactive panel sessions, and challenges presented to the Institute to ensure it stays on the leading edge of technology and policy. From the Opening Plenary to the close, attendees were provided a look into the future of nuclear materials management, and in the Closing Plenary, they were able to participate through a special interactive polling session to provide their own perspective of the future challenges that the world and the Institute will face.

The Second WINS Challenge

During the Opening Plenary[1] — in addition to two excellent speakers, Dr. Maria Betti and Dr. Brent Park — Will Tobey, the chair of the World Institute for Nuclear Security (WINS) provided a 10-year anniversary update of the activities of that international organization. Describing the INMM as the "father of WINS," he recounted how Charles Curtis had challenged the Institute in 2005 in the Opening Plenary of the 46th Annual Meeting to establish a new organization to develop and share best practices in nuclear security management. Our own president, Corey Hinderstein, and other members of the Institute participated in a Strategic Planning Group that took that challenge and established WINS as an internationally recognized organization in September 2008 in Vienna. Ten years later, there are over 4,700 members in more than 128 countries, and over 1,000 participants worldwide, in the WINS Academy, with 292 Certified Nuclear Security Professionals. WINS has hosted over 80 International Best Practices Workshops and produced 35 International Best Practices Guides. On this tenth anniversary, Will presented a new challenge to the Institute:

> *"By 2025, every person in this room, and every person worldwide who is employed professionally in the nuclear materials management, security, nuclear forensics, and safeguards fields will have the opportunity to take certified professional development courses to help demonstrate their professional competence."*

This new challenge, which WINS proposed to be supported by both them and INMM, is to the membership and their organizations to take the lead role. Fortunately, this is a strategic topic that has been discussed in the Executive Committee (EC) for the past two years, which culminated in a pilot professional development certification course offered to Annual Meeting attendees by Texas A&M University, entitled "Policy and Technical Fundamentals of International Nuclear Safeguards."[2] Sixty-seven attendees took advantage of this comprehensive online course, which was capstoned by presentations during a special four-hour session of international experts Sunday morning prior to the start of the Annual Meeting. In producing, organizing, and following through on this course, Dr. Sunil Chirayath[3] pioneered the concept that supported the new WINS Challenge. Now it is up to us to develop the relationships with external organizations, including our National Laboratories in the United States and other institutions and organizations worldwide, to make this a reality.

The Cyber Challenge

Tuesday evening the newly formed Cyber/Physical Security Integration Committee met to discuss newly developed bylaws and an agenda for the coming year. This new committee was the result of strategic discussions by the EC during the past year as the Institute, like much of the rest of the world, has been faced with cyber challenges. The new committee has been established as a temporary resource for the technical divisions to integrate relevant cyber- and cyber-physical-security concepts and applications in pertinent areas of nuclear materials management. Dave Lambert, who was a guest columnist for us in 2016 when he was working in Kazakhstan,[4] is the new chair of the committee, having returned to the United States as director of Gregg Protections Services, LLC. He has re-engaged with the Institute, having previously served as the chair of what is now the Nuclear Security and Physical Protection Technical Division, and he is now leading this new committee to ensure that cyber is integrated into all of the work of the Institute.

Since cyber issues impact all aspects of the Institute's mission, the EC believed it was important to establish this cross-cutting committee to work with all of the technical divisions to identify topics that impact them, encourage papers and workshops, and continue to provide value-added information for our membership. The importance of the cyber environment is, of course, around us every day, from identify theft at the personal level to efforts influencing national elections, disrupting infrastructure, and stealing state secrets and industrial technologies.

Most recently in the United States, we have seen the following indicators of how influential this issue has become:

- Standup of the U.S. Cyber Command (USCYBERCOM) as the U.S. 10th Unified Combatant Command on May 4, 2018. Originally established as a subcommand under U.S. Strategic Command, CYBERCOM is now at the same level as other unified combatant commands and will be led by a four-star general. The new command will include 6,200 personnel organized into 133 teams, including active service members as well as members of the Reserve and National Guard.[5]
- A new office of Cybersecurity, Energy Security, and Emergency Response (CESER) has been established in the DOE.[6] This new office will focus on energy infrastructure security, support the expanded national security responsibilities assigned to the Department, and report to the Under Secretary of Energy.
- On July 31, 2018, Homeland Security Secretary Kirstjen Nielsen announced the creation of a new center to share threat information with private companies at a Cybersecurity Summit held in New York City with several other high-ranking Administration officials and industry leaders, include Secretary of Energy Rick Perry. The National Risk Management Center is expected to provide a central location for cybersecurity solutions nationwide.[7]
- As regards the new NSA Cyber Operations Center, the National Security Agency and Cyber Command marked the official opening of a new $500 million building on May 4, one that is designed to integrate cyber operations across the U.S. government and foreign partners. The new Integrated Cyber Center and Joint Operations Center (ICC/JOC) is Cyber Command's first dedicated building, providing the advanced command and control capabilities and global integration capabilities needed to perform their missions.[8]
- Despite the complexities and resultant risks of the new cyber world, the DoD is moving toward cloud solutions for much of their data, including releasing a $10 billion request for proposals for the Joint Enterprise Defense Infrastructure (JEDI), which could potentially house nuclear weapons design data.[9]

In the international community, we have the following recent developments:

- NATO: At the Brussels Summit in 2018, Allies agreed to set up a new Cyberspace Operations Center as part of NATO's strengthened Command Structure.[10] Discussions are also underway to better define the level of cyberattack that would provoke a response under Article 5 of the NATO Charter, which is the alliance's principle of collective self-defense.[11]
- European Union: The EU is planning to enhance its cyber-resilience by setting up an EU-wide certification framework for information and communication technology (ICT) products, services, and processes.[12]
- Nuclear Threat Initiative: The Initiative has documented international cyberthreats in several reports, examining the vulnerabilities of nuclear material and facilities.[13]

As the world prepares for this new "battlefield," we will see this new committee engage with the technical divisions and open up new discussions, encourage papers, and facilitate panels for upcoming Annual Meetings.

The Challenges That Lie Ahead — Closing Plenary

An extraordinary Closing Plenary was held in Baltimore this year, moderated by then-President Corey Hinderstein (in her final year in that role), and designed to challenge the membership to think about the future of the Institute through a series of seven questions[14] created by the EC as a component of our new Strategic Plan. Stimulated by an international panel of five experts,[15] attendees were able to register their perspectives on remote polling devices, and results were documented to compare and contrast the perspectives of the five experts to the weighted perspectives of the attendees. Corey expertly coaxed feedback from the panel as well as from attendees to draw out the details of these perspectives. The results of this exercise will be used by the EC to help craft priorities for the Institute over the next couple of years, including a focus on future themes for the Annual Meeting.

This column is intended to serve as a forum to present and discuss current strategic issues impacting the Institute *of Nuclear Materials Management in the furtherance of its mission. The views expressed by the author are not necessarily endorsed by the Institute but are intended to stimulate and encourage* JNMM *readers to actively participate in strategic discussions. Please provide your thoughts and ideas to the Institute's leadership on these and other issues of importance. With your feedback, we hope to create an environment of open dialogue, addressing the critical uncertainties that lie ahead for the world, and to identify the possible paths to the future based on those uncertainties that can be influenced by the Institute. Jack Jekowski can be contacted at jpjekowski@aol.com.*

Endnotes

1. The Opening Plenary session this year was streamed live and is archived on YouTube (www.youtube.com/watch?v=Nh2vSK4gyVs&feature=youtu.be). The presentation and challenge by Will Tobey can be seen beginning at 1:40:30 of the video.
2. See https://nsspi.tamu.edu/nsspi-conducts-workshop-on-policy-and-technical-fundamentals-of-international-nuclear-safeguards
3. Dr. Chirayath is an associate professor in the Nuclear Engineering Department, director at the Center for Nuclear Security Science & Policy Initiatives, and an honorary professor at Amity Institute of Nuclear Science & Technology.
4. See Jekowski, J. 2011. Taking the Long View in a Time of Great Uncertainty: A View from the International Community, *JNMM*, *44*:4, 52–54.
5. See www.dodlive.mil/2018/05/03/cybercom-to-become-dods-10th-unified-combatant-command
6. Karen S. Evans was sworn in by U.S. Deputy Secretary of Energy Dan Brouillette as the Assistant Secretary for the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) on September 4, 2018. See www.energy.gov/ceser/ceser-leadership
7. See www.dhs.gov/sites/default/files/publications/national-risk-mgmt-fact-sheet-08282018-508.pdf and www.wired.com/story/dhs-national-risk-management-center
8. See www.fifthdomain.com/dod/cybercom/2018/05/07/cyber-command-nsa-open-new-500-million-operations-center
9. See www.nextgov.com/emerging-tech/2018/05/pentagon-wants-cloud-secure-enough-hold-nuke-secrets/148192
10. See www.nato.int/cps/en/natohq/topics_78170.htm
11. See www.nato.int/cps/en/natohq/topics_110496.htm
12. See www.consilium.europa.eu/en/press/press-releases/2018/06/08/eu-to-create-a-common-cybersecurity-certification-framework-and-beef-up-its-agency-council-agrees-its-position
13. See www.nti.org/media/documents/NTI_CyberThreats__FINAL.pdf and www.nti.org/analysis/reports/outpacing-cyber-threats-priorities-cybersecurity-nuclear-facilities. Also see https://ntiindex.org/news-items/important-nuclear-security-progress-now-in-jeopardy-according-to-2018-nti-index
14. Seven questions were provided to the panelists prior to the Closing Plenary, with several multiple choice answers, including "other." After asking the attendees for their input, the panelists and the attendees were queried for more details. The questions posed were: (1) What is the current top global challenge/risk/threat with respect to nuclear proliferation? (2) What is the current top global challenge/risk/threat with respect to nuclear security? (3) Which risk set concerns you more? (4) What are the greatest cyber threats related to nuclear materials management? (5) What are the top 3 areas the INMM should focus on? (6) Which technology has the best chance to become a "game changer" (plus or minus), for the INMM? (7) Where should the INMM increase its attention?
15. Panelists included Dr. Jacques Baute, Director, Division of Information Management, Department of Safeguards, IAEA; Dr. Bassam Abdullah Ayed Khuwaileh, Assistant Professor, Nuclear Engineering Program, University of Sharja; Mitsuo Koizumi, Manager of Technology Development Promotion Office of Integrated Support Center for Nuclear Nonproliferation and Nuclear Security of the Japan Energy Atomic Agency; Sonia Fernández-Moreno, Planning and Evaluation Officer, Brazilian-Argentine Agency for Accounting and Control of Nuclear Materials; and Julie Oddou, Head of the Committee Technique Euratom, Atomic Energy Commission (CEAR).

2018

INMM
INSTITUTE OF
NUCLEAR MATERIALS
MANAGEMENT

59th Annual Meeting

July 22-26, 2018
Baltimore Marriott Waterfront • Baltimore, Maryland USA

INMM Gratefully Acknowledges the 59th Annual Meeting Exhibitors, Sponsors and Advertisers

Sponsors

Mirion Technologies (Canberra)
Savannah River National Laboratory

Exhibitors

Aquila
H3D, Inc.
IAEA Careers
Idaho National Laboratory
International Safeguards Project Office/IAEA
Los Alamos National Laboratory
Mirion Technologies (Canberra)
Oak Ridge National Laboratory
ORTEC
Pantex Plant/Y-12 National Security Complex
PHDS Company
Quaesta Instruments
Razor Ribbon/Allied
Sandia National Laboratories
Savannah River National Laboratory

Calendar

January 22-24, 2019
INMM Spent Fuel Management Seminar — XXXIV
Hilton Alexandria Old Town
Alexandria, Virginia USA

March 3 - 7, 2019
Waste Management Symposia Annual Conference – WM2019
Phoenix Convention Center
Phoenix, AZ USA

March 12-13, 2019
Just Trust Me Workshop
Sandia National Laboratory
Albuquerque, New Mexico, USA

July 14-18, 2019
INMM 60th Annual Meeting
JW Marriott Desert Springs
Palm Desert, California USA

August 4-9, 2019
PATRAM 2019
New Orleans Marriott
New Orleans, Louisiana USA

July 12-16, 2020
INMM 61st Annual Meeting
Baltimore Marriott Waterfront
Baltimore, Maryland USA

For more information, visit the INMM Events Page.

Author Submission Guidelines

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

Submission of Manuscripts: *JNMM* reviews papers for publication with the understanding
that the work was not previously published and is not being reviewed for publication elsewhere. This restriction includes papers presented at the INMM Annual Meeting. Papers may be of any length. All papers must include an abstract.

The *Journal of Nuclear Materials Management* is an English-language publication. We encourage all authors to have their papers reviewed by editors or professional translators for proper English usage prior to submission.

Papers should be submitted as Word or ASCII text files only. Graphic elements must be sent in TIFF, JPEG or GIF formats as separate electronic files.

Submissions may be made via email to Managing Editor Amy Chezem at achezem@inmm.org.

Download an article template for the proper format for articles submitted to *JNMM* for possible peer review.

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

Format: All papers must include:

- Corresponding author's complete name, telephone number and email address
- Name and address of the organization where the work was performed
- Abstract
- Tables, figures, and photographs in TIFF, JPEG, or GIF formats. Color is preferred.
- Numbered references in the following format: 1. Jones, F. T., and L. K. Chang. 1980. Article Title. *Journal* 47(No. 2): 112–118. 2. Jones, F. T. 1976. *Title of Book*, New York: McMillan Publishing.
- Author(s) biography and photos
- A list of keywords

Download the article template from the INMM website.

The *Journal of Nuclear Materials Management* does not print "foot notes." We publish references and/or end notes. If you choose to include both references and notes, you may combine them under the same heading or you may keep them separate, in which case you must use numbers for the References (1., 2., 3., etc.) and letters (A., B., C., etc.) for the End Notes.

JNMM is published digitally in full color. Color graphics and images are preferred.

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

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

INSTITUTE OF NUCLEAR MATERIALS MANAGEMENT

60th ANNUAL MEETING

July 14-18, 2019
Palm Desert, CA, USA

JW MARRIOTT DESERT SPRINGS

www.inmm.org/Events/Annual-Meeting
#INMM19

CELEBRATING 60 YEARS

INMM
INSTITUTE OF
NUCLEAR MATERIALS
MANAGEMENT