UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

May 18, 2016

MEMORANDUM TO: ACRS Members

FROM: Christiana Lui, Technical Advisor
ACRS

SUBJECT: CERTIFICATION OF THE MINUTES OF THE ACRS RELIABILITY AND PRA SUBCOMMITTEE MEETING – USING VULNERABILITY ASSESSMENT TO IMPROVE SAFETY/SECURITY INTERFACE, APRIL 6, 2016, ROCKVILLE, MD

The minutes for the subject meeting were certified on May 17, 2016, as the official record of the proceedings of that meeting. Copies of the certification memorandum and minutes are attached.

Attachments: Certification Memorandum
Minutes
Meeting Transcript

cc w/o Attachments: A. Valentin
M. Banks

UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

May 17, 2016

MEMORANDUM TO: Christiana Lui, Technical Advisor
ACRS

FROM: Dennis C. Bley, Chairman
Reliability and PRA Subcommittee

SUBJECT: CERTIFICATION OF THE MINUTES OF THE ACRS RELIABILITY AND PRA SUBCOMMITTEE MEETING – USING VULNERABILITY ASSESSMENT TO IMPROVE SAFETY/SECURITY INTERFACE, APRIL 6, 2016, ROCKVILLE, MD

I hereby certify, to the best of my knowledge and belief, that the minutes of the subject meeting on April 6, 2016, are an accurate record of the proceedings for that meeting.

/RA/ **5/17/16**

Dennis C. Bley, Chairman Date
Reliability and PRA Subcommittee

Certified on: May 17, 2016
Certified by: Dennis Bley

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
MINUTES OF THE RELIABILITY AND PRA SUBCOMMITTEE MEETING

USING VULNERABILITY ASSESSMENT TO IMPROVE SAFETY/SECURITY INTERFACE
APRIL 6, 2016
ROCKVILLE, MD

INTRODUCTION

The Advisory Committee on Reactor Safeguards (ACRS) Reliability and PRA Subcommittee held a meeting on April 6, 2016, in room T-2B1, 11545 Rockville Pike, Rockville, Maryland. The Subcommittee was briefed by the NRC staff and other interested stakeholders on the security regulatory framework for nuclear power plants and planned activities to more explicitly incorporate vulnerability assessment results into NRC's physical security regulatory approach to improve safety/security interface.

The morning session convened at 8:30AM and adjourned at 11:47AM, and the afternoon session was closed to protect security information pursuant to 5 U.S.C. 552b(c)(1). See the meeting agenda below for specific briefing topics during the morning session. No written comments were received from members of the public related to this meeting. Mr. Marvin Lewis provided verbal comments during the meeting

ATTENDEES

ACRS Members
Dennis C. Bley (Chairman)
Charles H. Brown, Jr.
Michael L. Corradini
Harold B. Ray
Peter Riccardella
Gordon R. Skillman
John W. Stetkar

ACRS Staff
Christiana Lui (DFO)
Michael Snodderly
Andrea Valentin
Kathy Weaver

NRC Staff
David Aird, RES
Don Carlson, NRO
Arlon Costa, NRO
David Diec, NSIR
Rocky Foster, NRO
Alan Frazier, OCM/Svinicki
Melanie Galloway, NSIR
Robert Krsek, OCM/Baran
John Nakoski, RES
Mark Orr, RES
Joe Rivers, NSIR
Greg Schoenebeck, NRO
Nathan Siu, RES
Mark Thaggard, NSIR
Lucieann Vechioli

Other Attendees
Greg Bernard, DHS
B. Erie Brooks, NEI
Matt Bunn, Harvard (via phone)
AJ Clore, NEI
Mark Cunningham, Self
Steve Fogarty, ARES Corporation
Chris Guryan, ARES Security
Walt Kirchner, Self
Dan McCorquodale, Rhino Corps
Steven Mirsky, NuScale
Marc Nichol, NEI
Bob Scott, ARES Security
Dick Speer, NEI
Matt Talbot, Rhino Corps

A table of significant issues discussed during the meeting is provided below, as a guide to the attached transcript.

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
Reliability and PRA Subcommittee

Using Vulnerability Assessment to Improve Safety/Security Interface

Rockville, MD
April 6, 2016

AGENDA

Cognizant ACRS Member: D. Bley

Cognizant ACRS Staff: C. Lui, Christiana.Lui@nrc.gov, (301) 415-2492

TOPIC		PRESENTER	Time	Transcript Pages
I.	Opening Remarks	Dennis Bley, ACRS	8:30 – 8:40am	4-11
II.	NRC Management Introductory Remarks	Melanie Galloway, NSIR/DSP	8:40 – 8:45am	11-14
III.	Overview of the Physical Security Regulatory Framework, Vulnerability Assessment Approach and Safety/Security Interface	Joe Rivers, NSIR/DSP	8:45 – 9:45am	14-57
IV.	Proposed Consequence-Based Approach for SMR Security Regulations	Marc Nichol, Nuclear Energy Institute	9:45 – 10:15am	57-86
V.	Break		10:15 – 10:30am	
VI.	The Role of Modeling and Simulation in Risk-Informed Security Decision Making	Steve Fogarty, ARES Corporation	10:30 – 11:15am	87-127
VII.	Coping with Complexities of Vulnerability Assessment	Matt Bunn, Harvard Kennedy School of Government	11:15 – 11:45am	127-150
VIII.	Public Comment		11:45am – Noon	150-152
IX.	Adjourn		Noon	

- During the meeting, use 301-415-7360 to contact the ACRS Office.

- Presentation should not exceed 50 percent of the total time allocated for a given item. The remaining 50 percent of the time is reserved for discussion.

- Twenty (20) hard copies (2 B&W slides per page) of handout and fifteen (15) full-page colored copies of each presentation should be provided to the Designated Federal Official (DFO)/ACRS Contact 30 minutes before the meeting.

- One (1) electronic copy of each presentation should be e-mailed to the DFO/ACRS Contact 1 day before the meeting. If an electronic copy cannot be provided within this timeframe, presenters should provide the DFO/ACRS Contact with a CD containing each presentation at least 30 minutes before the meeting.

Significant Issues from ACRS April 6, 2016
Reliability and PRA Subcommittee Meeting
Issues linked to location in attached meeting transcript

SIGNIFICANT ISSUES	
Issue	**Reference Pages in Transcript**
Commission Directions	
• SRMs Regarding ACRS Focus in Security	8-9
• PRA Policy Statement	12
Regulatory Framework & Guidance	
• Design Basis Threat (DBT)	17-20
• Target Set	21
• Insider Mitigation	29-30
• Safety/Security Interface (Next Steps)	36
• Right Sizing the Required Protective Posture for Small Modular Reactors and Advanced Designs (Decision Metrics)	60-66 71-75
• Right Sizing the Required Protective Posture for Small Modular Reactors and Advanced Designs (Assessment Methods)	79-80
• Right Sizing the Required Protective Posture for Small Modular Reactors and Advanced Designs (Applicability to the Operating Fleets)	83-85
• Need for Regulatory Guidance on the Use of Modeling/Simulation Tools	120-123
Methodology	
• Similarities and Differences between PRA and Vulnerability Assessment (Use of Risk Triplet & Terminology)	6-7 23-24 94-100
• 4 Ways to Conduct Vulnerability Assessment	40-41
• Modeling/Simulation Tools: Pros & Cons	129-131
• Safety/Security Interface (Target Sets & Cut Sets)	21 55 96-97
• Safety/Security Interface (Example)	33
• Physical & Cyber Security Interface	146
• Modeling Human Performance (Adversary & Response Force)	99-101 108-110
• Modeling Pathway	103-107
• Modeling: Level of Detail to Support Decision-making	123-126
• Estimating Risk – Initiating Event Frequency & Conditional Risk	22-23 26-28 98
• Estimating Risk – Assumption, Quantification, Data & Validation	41-47 124
• Y-12 Modeling Issues	113-114 133-135
Review & External Engagement	
• Peer Review of Staff's Work	31
• External Engagements	39
• Compiling Database on Security Lessons-Learned	142

DOCUMENTS PROVIDED TO THE COMMITTEE

1. U.S. Nuclear Regulatory Commission, "Staff Requirements (M031002) - Meeting with Advisory Committee on Reactor Safeguards (ACRS), 9:30 A.M., Thursday, October 2, 2003, Commissioners' Commissioners' Conference Room, One White Flint North, Rockville, Maryland (Open to Public Attendance)," October 31, 2003 (ML033040278).

2. U.S. Nuclear Regulatory Commission, “Staff Requirements – SECY-06-0204 – Proposed Rulemaking – Security Assessment Requirements for New Nuclear Power Reactor Designs,” April 24, 2007 (ML071140119).

3. U.S. Nuclear Regulatory Commission, "Staff Requirements (M081217B) - Affirmation Session, 1:55 P.M., Wednesday, December 17, 2008, Commissioners' Conference Room, One White Flint North, Rockville, Maryland (Open to Public Attendance) (M081217B)," December 17, 2008 (ML083520252).

4. U.S. Nuclear Regulatory Commission, “Nuclear Power Plant Security Assessment Guide,” NUREG/CR-7145, April 2013 (ML13122A181).

5. D.W. Whitehead, C.S. Potter and S.L. O’Connor, “Nuclear Power Plant Security Assessment Technical Manual,” SAND2007-5591, Sandia National Laboratories, September 2007 (ML072620172).

6. U.S. Nuclear Regulatory Commission, “Regulatory Guide 1.174 – An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” Revision 2, May 2011 (ML100910006).

7. Nathan Siu, “Risk-Informed Security: Summary of Three Workshops,” presentation at the Joint INMM/ANS Workshop on Safety-Security Risk-Informed Decision-Making, April 26, 2015, Sun Valley, Idaho, U.S.A. (ML15116A004).

8. Steve Fogarty, “Defining the Analysis Scope to Support Decisions While Ensuring the Technical Acceptability of the Results,” presentation at the Nuclear Regulatory Commission Regulatory Information Conference, March 8-10, 2016, Rockville, Maryland, USA.

9. Christopher Kelley, Rob White, Bill Guthrie, “Computer Modeling,” presentation at the Nuclear Regulatory Commission Regulatory Information Conference, March 8-10, 2016, Rockville, Maryland, USA.

10. Joe Rivers, “Risk Informing Security,” presentation at the Nuclear Regulatory Commission Regulatory Information Conference, March 8-10, 2016, Rockville, Maryland, USA.

11. U.S. Nuclear Regulatory Commission, “Security Regulatory Framework for Certifying, Approving, and Licensing Small Modular Nuclear Reactors (M110329),” SECY-11-0184, December 29, 2011 (ML112991113).

12. Nuclear Energy Institute, "Position Paper – Physical Security for Small Modular Reactors," July 31, 2012 (ML12221A197).

13. Russell Bell, “Position Paper on Physical Security for Small Modular Reactors,” Letter to Michael Mayfield, August 1, 2012 (ML12221A201).

14. Nuclear Energy Institute, "White Paper - Proposed Consequence-Based Physical Security Framework for Small Modular Reactors and Other New Technologies," November 2015 (ML15349A244).

15. Russell Bell, “Proposed Consequence-Based Physical Security Framework for Small Modular Reactors and Other New Technologies,” Letter to Michael Mayfield, November 19, 2015 (ML15323A245).

Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
Reliability and PRA Subcommittee Meeting

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Wednesday, April 6, 2016

Work Order No.: NRC-2301 Pages 1-147

NEAL R. GROSS AND CO., INC.
Court Reporters and Transcribers
1323 Rhode Island Avenue, N.W.
Washington, D.C. 20005
(202) 234-4433

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

RELIABILITY AND PRA SUBCOMMITTEE

+ + + + +

WEDNESDAY

APRIL 6, 2016

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Subcommittee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B1, 11545 Rockville Pike, at 8:31 a.m., Dennis C. Bley, Chairman, presiding.

COMMITTEE MEMBERS:

DENNIS C. BLEY, Chairman

CHARLES H. BROWN, JR. Member

MICHAEL L. CORRADINI, Member

HAROLD B. RAY , Member

PETER RICCARDELLA, Member

GORDON R. SKILLMAN, Member

JOHN W. STETKAR, Member

DESIGNATED FEDERAL OFFICIAL:

CHRISTIANA LUI

ALSO PRESENT:

MATT BUNN, Harvard Kennedy School of Government*

STEVE FOGARTY, ARES Corporation

MELANIE GALLOWAY, NSIR/DSP

MARVIN LEWIS, Public Participant*

MARC NICHOL, NEI

JOE RIVERS, NSIR/DSP

*Present via telephone

T-A-B-L-E O-F C-O-N-T-E-N-T-S

P-R-O-C-E-E-D-I-N-G-S

(8:31 a.m.)

MEMBER BLEY: Good morning. The meeting will now come to order. This is a meeting of the Advisory Committee on Reactor Safeguards, Subcommittee on Reliability and PRA.

I am Dennis Bley, Chairman of this meeting. Members in attendance are Mike Corradini, Dick Skillman, Harold Ray, and John Stetkar. We may be joined later by Charlie Brown and Pete Riccardella. Christiana Lui of the ACR staff is the designated federal official for this meeting.

The purpose of the meeting is to receive an information briefing on the security regulatory framework of nuclear power plants, and planned activities to more explicitly incorporate vulnerability assessments into the NRC's physical security regulatory approach to improve safety/security interface.

The subcommittee will hear presentations by, and hold discussions with representatives from NRC's Office of Nuclear Security and Incident Response, the Nuclear Energy Institute, ARES Corporation, and the Kennedy School of Government at Harvard University.

The subcommittee will gather information, analyze relevant issues and facts, and formulate proposed positions and actions as appropriate for deliberation by the full committee.

I think we'll begin with a little history. Vulnerability assessment has been in development and use for applications in the physical security area since the 1970s. Over the last several decades the methods, data, and subsequent computer based modeling and simulation tools have continued to evolve based on the needs, operating experience, and technology advancement.

Other federal agencies, such as the Department of Defense and the Department of Energy have sponsored the development of vulnerability assessment software tools, and used the results in the design and evaluation of protection strategies for sites, facilities, or materials under their jurisdictions.

As the desktop computing power grew, the modeling simulation software that used to require multi-station, multi-analysts, migrated onto portable computing platforms.

Within the NRC the Office of Nuclear Security and Incident Response, NSIR, and the

Office of Regulatory Research, have participated in or sponsored workshops that focused on safety/security interface and risk informed decision making, since about 2010.

Last year I had the opportunity to attend the Joint Institute of Nuclear Materials Management, and the American Nuclear Society Workshop at Sun Valley. And the Committee sponsored me to attend a subsequent workshop in Boston.

Based on my observations both the vulnerability assessment and PRA in the safety area use the Tripwood approach. I'm going to go off script for a minute.

I spent, before I got on this committee I spent several years working with a group under the Gen 4 Program, looking at proliferation resistance and physical protection, trying to develop methods in that area.

And it took us over two years to just get past the language barriers between safety people, risk people, physical protection people, and proliferation resistance people. In the end, pretty much everybody agreed that the problems we were solving were very related.

And they really had to deal with the fact that barriers and protection systems, and the like, don't have intrinsic value. They have value that's very much scenario based. And for one scenario a particular barrier might be very good, for another not so good.

And that this idea of a scenario based kind of analysis, and we even had to change the words a little bit so everybody could be comfortable, the pathways approach, really seemed to anchor where we were headed. The same things we're seeing here a bit.

Although the quantification processes and certain modeling aspects are different among these analyses, there are many opportunities to leverage the similarities between a vulnerability assessment and say a PRA to improve the safety/security interface, and better facilitate efficiency and effectiveness.

Additionally, I understand several operating nuclear power plant fleets, Xcel Energy, PSEG, and Exelon are using the commercially available modeling simulation software to model, assess, and adjust their site protective strategy.

In fact, two sites have submitted

proposed changes to their physical security plans to the NRC for review, using the modeling simulation results as part of the support for the proposed changes.

On the advanced designs and small modular reactors front, in November 2015 Nuclear Energy Institute submitted to the NRC a White Paper, "Proposed Consequence Based Physical Security Framework for Small Modular Reactors and Other New Technologies", which advocates a more explicit security regulatory framework that uses risk insights for SMRs. We will hear more about that this morning.

I think, to put a little perspective here, I'd also mention several SRMs that have been issued over the past many years. There have been I think at least three or four that I remember, that has urged the staff to integrate safety/security to the extent possible.

Back in 2003 an SRM on, following a meeting with this committee, our parent committee, the Commission said on the security area, ACRS should continue to focus its attention and expertise on technical issues associated with the progression and potential consequences of

postulated terrorist actions, and the assessment of mitigation strategies.

And later, in 2008, in an SRM on SECY-08-0099, Final Rule, Power Reactor Security Requirements, they said the staff should have the Advisory Committee on Reactor Safeguards review the implementation guidance for portions of the rulemaking with the committee's scope.

The rules for participation in today's meeting has been announced as part of the notice of this meeting previously published in the Federal Register on March 23rd, 2016. A transcript of the meeting is being kept, and will be made available as stated in the Federal Register notice.

Therefore, we request that participants in this meeting use the microphones located throughout the meeting room when addressing the subcommittee. Participants should first identify themselves, and speak with sufficient clarity volume so that they may be readily heard.

Also, for all of the folks at the tables, the desk microphones have a little button on the front. Please push that when you're going to talk, and turn it off when you're finished. Having them on all the time interferes with, it

creates noise for the people on the phone listening in.

It's requested that presenters first identify themselves. Also, given the nature of today's topic, the presenters should stop the discussion if the content can no longer be discussed in a public forum. And we'll have to leave that up to you to be careful.

We will adjourn this morning's sessions promptly at noon. We have another meeting scheduled then. So we'll have to finish the full agenda for this morning by noontime. And we'll return for a closed session with the committee after lunch.

We ask at this time that you silence your phones and other electronic devices. Although we have a bridge line open to preclude interruption of the meeting, the phone bridge will be placed in the listen in mode only during the, it will be in the listen in mode only during all presentations and committee discussion.

We'll open the phone line late in this open meeting to allow public comment. Prior to today's meeting we have received no written comments or requests for time to make oral

statement from members of the public regarding today's meeting.

We will now proceed with the meeting. And I call upon Melanie Galloway, Director of the Division of Security Policy, in the Office of Nuclear Security and Incident Response, to begin. Melanie, please.

MS. GALLOWAY: Okay. Thank you very much, Chairman Bley. First of all from a personal standpoint I'd like to say how pleased I am to be back before the ACRS. It's been some time since my ACRS interactions on license renewal. And it's good to see you all again.

I'm pleased to be here to introduce this topic, and particularly to give a little bit more information regarding the NSIR work in this area, and to introduce Joe Rivers.

As Chairman Bley has mentioned, the idea of risk informed security has been gaining momentum over the last several years, in particular the last four or five.

This is part of an overall activity that NSIR is involved in to risk inform. We're taking a leadership role in that regard, both domestically, and doing some international

leadership work as well.

It goes without saying that when we talk about risk informing anything we need to reflect on the fact that there is a Commission policy statement that has to do with the use of PRA methods in regulatory activities.

And in that policy statement it explicitly points out that all regulatory matters should be further risk informed. And while certainly the risk informing activity by the VA tools is not a PRA, per se, the use of such tools is certainly within the spirit of that Commission policy statement.

As Chairman Bley mentioned, we have conducted a number of workshops. In particular, last year we conducted two with the ANS, and with the Institute of Nuclear Materials Management, in which Joe Rivers did provide a leadership in those workshops, and provided discussion in order to get a dialogue going about what are the various ways that can be risk informing in the security realm, and also to talk about the safety/security interface, and what information we can gain and apply to our work, both on the part of licensees, as well as the NRC.

In these workshops we have noted an increased attention and attendance by industry folks, as they are seeing the value in risk informing their security activities.

The use of modeling and simulation, we call it Mod Sim, should support better decision making. And that's clearly what everyone is looking for.

You know, the industry has its priorities in terms of the decision making that can make more effective use of their resources. And we too have perspectives, in terms of how the values of these tools can better inform our regulatory activities.

And they're not always aligned, but they do come at it from the same perspective of, what can we gain, and how can we best use this material? And certainly we're here to talk to you today about the safety/security interface, which is very much fitting in with your safety focus.

And that's an area as well that we're doing a lot of work in. Right now it's a little bit of an extension of what we do, because we're focusing primarily on the security piece. But understand that the safety/security piece is

important to us as well.

Joe Rivers is going to provide a little bit of a regulatory framework about how the VA tools fit in with our security licensing process, as well as talk about the tools themselves, and then get into some safety/security interface. So with that, I'll turn it over to Joe.

MR. RIVERS: Okay. So, Chris asked me to sort of lead into the discussion today, so that the members of the subcommittee would have a better understanding as the later presentation is rolled out. So how it all fits into this framework.

How do I make this thing go down? Page down. I hit page down. It doesn't work.

PARTICIPANT: Try hitting the space bar.

MR. RIVERS: Space bar? No.

(Off microphone comments)

MR. RIVERS: I tried page down. That doesn't work. Now it does. Okay.

(Off microphone comments)

MEMBER STETKAR: It's good you could learn something here this morning. This is, you know, a fallout of Project Aim. You are now trained --

MR. RIVERS: I just had to make sure that my --

MEMBER STETKAR: -- to do this in any medium.

MR. RIVERS: My former boss is here to get things started. So, okay, we're going to cover a number of topics in the next hour. And feel free to interrupt at any time if you've got questions on any specific issues there.

We'll talk about the physical security regulatory framework, a little bit about safety/security interface. I'll give you some background on some of the activities we've had on risk informing security that Dennis mentioned earlier, and also Melanie.

And then I'll talk a little bit about what vulnerability analysis is, and what some of the different tools are, to lead into later discussion today.

So, NRC's power reactor security program, it's really there to provide high assurance of adequate protection to prevent significant core damage with spent fuel, and spent fuel sabotage. So it's designed to protect against the design basis threat, in order to prevent

radiological sabotage.

And the process is for NRC to develop licensing and inspection programs, as well as industry initiatives that implement and verify the level of protection described. So the real focus is to protect against radiological sabotage as defined in the design basis threat.

There's a lot of individual requirements, both prescriptive and performance based throughout the regulations. But in the end the idea is to protect against radiological sabotage.

If we look at how we get moving, we have licensing for operating nuclear power reactors. And 10 CFR 50 and 73 regulations apply. And there's also a formalized process to make changes.

For new reactors we have 10 CFR 52 and 73. There's also a final safety analysis report which must describe the engineered physical security programs, and implement security requirements before fuel is allowed inside the protected area. So, before the fuel actually arrives onsite, the security measures have to be in place.

The NRC also uses NUREG-0800, the Standard Review Plan, and various regulatory guides to conduct security plan reviews and approvals. Security plans tend to be sort of the foundation of how security operates at the facilities, and also with our regulatory oversight and responsibilities.

They provide a physical protection against the design basis threat. They establish and maintain a physical protection system and security organization. They establish and maintain at all times properly trained, qualified, and equipped personnel that are required to interdict and neutralize the threats.

The requirements can be found in 10 CFR 73.55 and 73.54. There are four basic types of security plans, the safeguard contingency plan, which is, if something happens, what are the, what is the protective force supposed to do?

Training and qualification plan. What makes a security protective force officer actually qualified. Physical security plan that sort of covers the spectrum of all the requirements and documents, how the program operates. And then in the recent years, cyber security plan.

MEMBER SKILLMAN: And, Joe, if you can,

is there a unique and specific definition of design basis threat in the context of the vulnerability assessment?

MR. RIVERS: Essentially what you have in the vulnerability assessments is the NRC proscribes the design basis threat. There's a sort of a general statement that you'll find in the regulations. And then the reg guide, I believe the one that applies for nuclear power plants at the radiological sabotage, which is --

MS. GALLOWAY: 5.69.

MR. RIVERS: -- 5.69. Actually, it's currently under revision right now. But that provides all of the adversary characteristics.

And so, when the utilities are in the process of conducting these vulnerability assessments, they will essentially populate the modeling program with all of the characteristics of the adversaries. And essentially allow the adversaries to attack the facility in the Mod Sim programs.

MEMBER CORRADINI: So, can I ask, since I don't know anything about this, but I'm curious. Is the DB, is the group of DBTs determined by just engineering judgment? Or is there a process?

MR. RIVERS: There's a distinct process. Essentially our office has the Intelligence Liaison and Threat Assessment Branch, which is our linkage to the intel community which brings information in, evaluates it.

Our office provides recommendations to the Commission when we believe the design basis threat should be changed. So, a lot of it's based on, you know, threat information we receive from the intel community.

There are decisions that have to be made as to whether or not something happening in Iraq could migrate itself to the United States. We will make recommendations to the Commission, and the Commission in the end is the one that decides whether something is added to the design basis threat or not.

MEMBER CORRADINI: But you make the recommendation?

MR. RIVERS: We make the recommendation in our office.

MEMBER CORRADINI: So maybe this isn't the right place to --

MEMBER BLEY: I think that's right.

MEMBER CORRADINI: Okay.

MEMBER BLEY: We shouldn't pursue this one much further.

MEMBER CORRADINI: Okay. I figured he'd stop me.

MR. RIVERS: Okay.

MEMBER CORRADINI: Thank you.

MR. RIVERS: So, our process of oversight of course is through an inspection program. We have two basic types of inspection. One is the baseline inspection, which covers a broad variety of topics.

And then one that tends to have a lot more visibility is the force-on-force inspection programs. The force-on-force actual graded inspections are once every three years at each of the nuclear power plants.

The actual operators of the facilities conduct training versions of these force-on-force four times, generally four times a year. NRC observes at least one of those, in addition to the once every three year graded exercise.

Special inspections are done based on things that may have happened at the plant, and the determination that we need to have a special inspection.

Safety/security interface, there is a requirement that's codified in 10 CFR 73.58, that safety/security interface requirements for nuclear power reactors. It applies to all operating nuclear power plants.

It requires a pre-assessment and management of all planned and emergent activities involving changes to plant configurations, facility conditions, and/or security programs. It requires to communicate potential conflicts to appropriate personnel, and take necessary actions to maintain safety and security, in accordance with NRC requirements and license conditions.

So this is the regulatory discussion. The next two slides I'll talk about sort of the value of it, and some of the things that I think are useful in that area.

One of the things to keep in mind, if we look at what are the target sets that are used in vulnerability assessments, and also in force-on-force inspections, they're actually derived from the cut sets from PRAs to inform the target sets.

So we use the PRA analysis to actually identify what targets might the adversaries actually hit to actually cause the core damage and

radiological sabotage.

Security vulnerabilities and associated consequences are needed by safety organizations to inform safety programs. So if the safety organizations don't know what might happen as a result of an adversary attack on a facility, they are not necessarily going to be able into place the proper safety and mitigation systems to protect that facility.

We also need to understand the relationship between safety and security risk. One of the things that, when we look at risk and we look at PRAs, PRAs we have all of these engineering values that say that there's a certain ten to the minus six probability that something is going to happen. And all of these numbers are based on engineering calculations. And some of it's based on judgment calls by experts.

In the security world you have a, fairly commonly you hear that we assume the adversary's going to attack. And so, the probability of attack is one. I tend to, as a statistician I tend to not like to look at it that way.

Although the safety community is

looking at the risk if something happened, in the security world what we tend to look at is what I would call the conditional risk. If an attack happens, how well do the security systems actually work? So, it's just a different perspective.

MEMBER CORRADINI: So, in the range of, so just back to other terminology. So, I don't remember the words you used. But the initiating event is assumed to be one?

MR. RIVERS: Well, that's what people talk about. But essentially, in reality what you're doing is, I'm taking a conditional risk. If that attack happens, what is the likelihood that the security systems are going to work?

MEMBER CORRADINI: And then all of the, as you had said, given that conditional --

MR. RIVERS: Given the --

MEMBER CORRADINI: Given that conditional starting point --

MR. RIVERS: Right.

MEMBER CORRADINI: -- you used PRAs to determine what might be --

MR. RIVERS: It's something very similar to PRAs. If you go back into, you know, the earliest days, the security vulnerability

assessments were probably some of the first modeling and simulation that was actually developed at the National Laboratories. And those same statisticians were the ones that actually developed the initial PRA models as well.

MEMBER CORRADINI: Okay.

MR. RIVERS: So given that it was the same people developing both tools initially, you're going to have a lot of similarities in the software.

MEMBER CORRADINI: Okay. Thank you.

MR. RIVERS: So, essentially we assume that, we basically say that our analysis in security is a conditional risk. That if an attack happens, what is the effectiveness of the security system?

Your sort of have to do that, because it's much, harder to identify the likelihood that an adversary is going to attack. If not random -- We really haven't had too many of them, none of them at nuclear facilities.

And a lot of it is based on adversary seeing that something is deficient at a plant, so I have an opportunity to do a much better job to attack. So they just don't randomly roll dice and

say, I'm going to hit this facility. They're actually assessing the facilities, and making determinations as when it's best to go.

And if we go, the other part, to understand the relationship between safety and security. I know talking to some of the security managers in facilities, one of the things that you find is that when they're trying to decide how much, how to spend their money to make sure that their reactor operates safely and securely, it becomes quite a challenge when we measure risk differently in the safety world and the security world.

And it would be much better if in the end we could achieve an understanding of how that safety risk relates to the security risk, so that the owners of these reactors can actually better risk inform their decisions on how to spend the money they have to protect that facility.

MEMBER BLEY: And you just hinted at it though, but didn't go in some. Some things you might do to improve security could actually hamper safety.

MR. RIVERS: That's right.

MEMBER BLEY: And vice versa.

MR. RIVERS: That's correct.

MEMBER BLEY: Yes. And that's the things we really would like to keep an eye on if we can.

MR. RIVERS: That's right.

MEMBER CORRADINI: And that currently is, just to make sure I understand. That currently is looked at by the licensees?

MR. RIVERS: Well, the licensee, because we don't really understand what that relationship is. And I know that a couple of the initiatives that have been briefed to this subcommittee and the full committee, like the risk prioritization initiative, and some other things, have talked to the fact that, yes, we're, you know, industry and NRC staff are trying to understand how those risks may be related.

We really don't have the answer yet. And I think it's something that in the end it probably would be of value to both the NRC and industry to have that understanding.

MEMBER CORRADINI: I'm sure that John and Dennis know this. But I just, I'm still struggling. So, since as a conditional situation where you're assuming that this whatever chooses to

be the thing that happens, happens, can you really ever do a comparison?

MR. RIVERS: Well, I think, you know, there have been, there are a lot of activity going on in the DoD world, and also, probably more so the DoD world, trying to understand the terrorist likelihood of attacks, the intel community.

And I think probably initially you probably want to do some sort of a semi qualitative, where I put it in some sort of a range.

MEMBER CORRADINI: So, in other words, there is some thought to essentially binning these assumed things into very large bins of likely, less likely, not so likely.

MR. RIVERS: I think there's been a lot of work in that area. I think that in the end that's where you have to start. Hopefully we never see an attack at a facility. And then we never have any empirical data. But I think initially you have to look at some sort of a binning process.

MEMBER CORRADINI: So, last question. Is there philosophically resistance by other parts of the Government to even think like this?

MR. RIVERS: I don't think there's any

resistance. I think people look at it as such a challenge to solve that not a substantial amount of work has been done in this area.

MEMBER BLEY: There's another side to it that, at least that has struck me whenever I've played with this concern. For the most part, from the safety side and the PRA side, the likelihood of a challenge is kind of constant thing.

In this area the likelihood of a challenge may not be, and may be changing. There are Government agencies that, Jeff said, that interact with NRC, that talk about threat level is changing day by day, week to week, or whatever. But it's probably not a constant.

MEMBER CORRADINI: So the risk is a dynamic concern? The risk is dynamic?

MR. RIVERS: The risk is very dynamic. You know, other things to keep in mind is there are other factors that are also hard to quantify. For example, what is deterrent scale?

If we look at our nuclear power plants in the U.S., we probably have some of the best, well guarded facilities in the world. If they were less well guarded, it might be adversary want to be attacking them more frequently. And so, even the

level of deterrence factors into the likelihood of an attack.

MEMBER BLEY: Because it's a choice, rather than a roll of the dice.

MR. RIVERS: Right. So --

MEMBER SKILLMAN: Joe, you made a comment that speaks loudly to me, several minutes ago. And that had to do with, when there's been a change that presents a vulnerability in the plant.

MR. RIVERS: Right.

MEMBER SKILLMAN: Let me back up. I've watched force-on-force for years. I've got a pretty good appreciation for how effective that security force anticipates and responds.

At the same time, the greater risk, at least in my judgment from being around these plants for decades, is the inside threat. The disgruntled employee, or the individual who can connect the dots and say, since we have that diesel down and that transformer out, or whatever that might be, this I the time.

What consideration is given to that more subtle, and perhaps deeper infection that's so difficult to dig out?

MR. RIVERS: We have, you know, a lot

of requirements for insider mitigation programs, to include behavioral observation programs. And then when we're considering, for example, in the force-on-force exercises, essentially you have an insider adversary that participates and provides complete information.

So, we do test the fact that, okay, if you do have an insider, what's going to happen? You know, insiders can also do more things. They can damage parts of the facility. They can, you know, make it easier for an adversary to get in.

There's a lot of things they can do. We may not test all of those. But those are things that the facility has to protect against. And insider activities are definitely real.

If we look at the Doel Reactor in Belgium, where they drained fluid from some system that ended up costing millions of dollars to repair, and lost revenue of millions of dollars as well, the insider adversary is something to be concerned about.

MEMBER SKILLMAN: Thank you, Joe.

MR. RIVERS: Sure.

MEMBER CORRADINI: If the Chairman will allow me? So, who are the peers that reviews what

you choose to do?

MR. RIVERS: What do you mean the peers that review?

MEMBER CORRADINI: Well, I mean, so to put it a different way. So, we're listening to this now. But all the front end of all of this is not our expertise. So somebody has that expertise that must peer review what you do, or what the group does.

Is there other parts of the intelligence community that says, yes, that sounds reasonable, or this seems unreasonable, or this is too much, this is too little?

MR. RIVERS: Well, we have a lot of interaction with our, the other agencies that protect this type of material, for example, the Defense Department and Department of Energy.

We have a lot of engagement with you all here this afternoon from the Director of the Office of Security at Department of Energy. And his organization is one of the ones that we engage with frequently.

MEMBER CORRADINI: But if I switch over to chemical or biological is there, I still have associated safety consequences.

MR. RIVERS: That's correct.

MEMBER CORRADINI: Or a consequence, I should say, due to the assumed whatever.

MR. RIVERS: Yes. And we, you know, we do look at chemical hazards at these facilities as well, both from a safety and security stance side as well.

MEMBER CORRADINI: Okay.

MEMBER BLEY: I'll just remind all the members, today is an information brief. And we have tons of topics. So I don't want to stifle questions. But we don't want the introductory one to get into the meat of the rest of the program.

MR. RIVERS: Yes. So one of the fundamental reasons for safety/security interface is one that Dennis mentioned as well. Is the need to evaluate impacts on each discipline as changes in the plant configurations or operations are planned.

So you don't, if I'm a security organization, you know, we go to the fundamental principles. In the security organization I try to lock all the doors. In the safety organization they try to unlock all the doors.

And so, the two disciplines have to

work together to achieve a balance between safety and security. And that's one of the real fundamental reasons for safety/security interface.

MEMBER BLEY: And that simple example we actually had happen early on.

MR. RIVERS: Right, yes.

MEMBER BLEY: Doors were locked, and safety guys couldn't get to the rooms they needed to.

MR. RIVERS: Yes. I'll give you an example. At one of the Category 1 facilities, when they were building the Great Wall of Erwin, which was a large wall around the facility, the preference by the security organization was to have one opening.

And safety said there had to be two. And so, those discussion go on. And essentially, in the end we're much better off when both safety and security both work.

So we also need to understand how information from each discipline can better inform the other discipline. And I think that's a lot of what we want to understand as well.

When, you know, we, the security world uses the information from the PRAs to support, you

know, identifying target sets, the safety world needs to understand what can happen if an adversary actually attacks, to make sure the proper safety and mitigation systems are in place. So, in the end the two disciplines have to work very closely together.

Risk informing security. Dennis mentioned and Melanie mentioned the fact that we've worked on a number of workshops. We had an initial workshop in 2010, hosted by Sandia National Laboratories.

Due to budget cuts I shifted the focus to getting professional societies to organize them. We ended up only having to pay registration fees, which makes it a lot more cost effective for NRC.

With, the INMM Stone Mountain workshop was actually a follow-on to the Sandia workshop. Both of those workshops were focused on trying to identify what some people might call low hanging fruit, as to, you know, what are the best areas to focus our attention on early on.

I also hijacked an INMM reducing risk workshop in March of 2015 to try to get better insights into risk informing security. And then in the spring and fall of 2015 the two workshops that

Dennis mentioned earlier started focusing on some of the things that had been identified in the earlier workshops.

Sun Valley workshop was focused on the safety/security interface. We actually took advantage of a meeting that ANS was hosting in Sun Valley on probabilistic risk assessments. And then set the meeting up on the Sunday prior to that meeting. And got security folks through the INMM to actually participate. So we actually had a pretty good engagement, about 30 to 35 individuals.

Then in the fall we had a workshop in Boston hosted by the Institute of Nuclear Materials Management. And it was really focused on VA tools. That it talked about the history of them, what some of the basic aspects of it.

We brought in an actual project I'd shared at the IEA on nuclear security assessment methodologies, where they developed a case study. And that case study was evaluated by each of the three vendors to give people an indication of what each of the tools actually does on a similar facility, essentially.

If we look at some of the things that, activity we have ongoing in risk informing

activities for nuclear power plants, we're all, we're looking at the use of modeling and simulation tools.

So that aspect we're, you know, trying to host workshops. We're trying to, or the staff is trying to understand how that can be incorporated in the regulatory framework.

Most of the staff doesn't have a lot of experience in this area. So I've been doing some internal workshops, trying to help the staff understand what this concept is, and how it can be used and incorporated in the regulatory framework.

Safety and security risk. I know that several of the participants at the Sun Valley workshop were NRC staff. And there's been a lot of discussion amongst the senior level advisors of trying to get some working group established to try to sort of come up with ideas of how to better do safety and security interface, and take advantage of that within the agency itself.

Cyber security. As that program was implemented when we got to the balance of plant area, we're interfacing with a grid. A lot of those critical digital assets, and those, that area are not heavy into the safety impacts.

And so, that concept of looking at potential consequence, which is risk informing, helped to better define what the requirements ought to be in a more graded program.

And then I mentioned earlier the IEA coordinated research project on nuclear security assessment methodologies. It's been ongoing for about three years.

The concept is to essentially develop a methodology for assessing the effectiveness of a security program at a wide range of facilities, to include things like a nuclear power plant, an irradiator facility, and independent spent fuel storage installations.

So, looking at the broad spectrum of facilities, and how do I actually determine the effectiveness of security. And as I said, the case study for the nuclear power plants was actually used at the Boston workshop.

Then we can look at a couple of industry initiatives. We mentioned earlier the risk prioritization initiative, which was both an NRC and an industry initiative.

But we also, in the last roughly half year, we've received a couple of submissions on

security plan changes that are 50/50/4P changes, which basically state that we're making a change in the security program. However, there's no change or reduction in the effectiveness of the security program.

Those submissions were supported by modeling and simulation, the VA tools. And we as a staff now are trying to determine how to use that analysis that was submitted to essentially validate the submissions of the industry. And so, that's sort of the initial steps of the process.

We'll have to, in end, between industry and NRC probably issue a number of guidance documents to better understand how that process needs to work.

Also, something you'll hear from the next speaker is the consequence based approach for SMR security regulations. And I won't talk too much of this.

But the NRC received their White Paper, industry's White Paper. And are, currently have it under evaluation. But you'll hear more about that White Paper from the next speaker. Yes.

MEMBER CORRADINI: So, is there stakeholder feedback on a lot of this as this

proceeds? Or are these workshops that you were speaking about, the first, wherever they were, on Slide number 10.

MR. RIVERS: Yes.

MEMBER CORRADINI: Are they the first ones where you get stakeholder, from the fleet, and how they're dealing with -- Given --

MR. RIVERS: We used to have to sort of open up the discussion. I think that I've tended to find that if we get on a neutral ground that sometimes that allows people to be more frank and open in their discussions.

Also, at these workshops it also had value that we had external stakeholders that are not industry and not NRC, to include the National Laboratories, and some of the university types that don't necessarily have a vested interest in what we're doing, that can talk about their experiences and their ideas on how to do things better.

MEMBER CORRADINI: Okay. Thank you.

MR. RIVERS: So, I've tried to take advantage of those outside organizations, to try to foster a better dialogue between industry and NRC. So, the question is, what is a vulnerability analysis?

It's a systematic performance based process that is used to evaluate the ability of a physical security system to meet its performance requirements. So, how well does that system work?

You know, if we look at what VA tools are, you know, there tends to be a focus that, if I'm using a VA tool it's that modeling and simulation program, that computer simulation.

In reality, there are a number of types of VA tools. If we look at tabletop analysis, that's probably the most simple and straightforward one that's probably used. And has historically been used by this industry, the nuclear power plant industry.

A lot of them have very interesting tabletops. I know if I went to the Lynchburg facility, they actually have, had a former model railroader that actually built his model of the facility. Very impressive. Some of them are just made out of cardboard.

But tabletops have been around for a long time in this industry. And I think we miss the point when we don't consider those vulnerability assessment tools, because they very much are vulnerability assessment tools.

Then the one that you'll hear more about today is the computer simulations. Dennis talked about the fact that these have, really were started probably in the 1970s, and have developed ever since.

And then we have some more labor intensive type ones. The limited scope performance test, where we want to test an element, or a system or subsystem of a protection system. We'll run an exercise on a portion of the actual overall physical protection system.

And then we have the ones that are force-on-force exercises. And those are also vulnerability assessment tools. They're probably the most expensive to get a single run. But they all are part of the vulnerability assessment process.

MEMBER BLEY: Joe.

MR. RIVERS: Yes.

MEMBER BLEY: I might be jumping the gun, but I want to ask a couple of related questions about this group of things. And when you look at a tabletop I think you can understand the model, what's going on and what you're doing.

When you get into computer simulations

you see what comes out. How do you as a regulator, if you look at these, understand the validity of what's coming out of the models? I'm not, I guess I'll get more familiar with limited scope performance tests. You might mention something about that.

And then the thing that kind of struck me at these workshops I went to is, you know, and this is true for safety too. We don't have very many core damage events, so that we can look at those and learn from them. And we don't have many attacks. And certainly none on our nuclear plants that we can look at.

But I heard a lot from the people doing computer simulations, and the people who might use them, that the way we confirm that these models are accurate is by looking at force-on-force exercises as data, which really struck me as uncomfortable.

Because they are at least to some extent stylized, with a set of rules. And they aren't, it might be the only data you have. But it's not completely applicable to the real world.

MR. RIVERS: Well, I think that the reason that people talk about the fact that force-on-force exercises gave them comfort, and what

they're saying are the results of the performance, you know, the results from the VA tools about the computer simulations is that that's what they're comfortable with. That's what they're familiar with.

And so, I think that you're going to see when that's their experience base, that's the thing that they try to relate to. I think that --

MEMBER BLEY: Which brings in some dangers.

MR. RIVERS: It brings in some danger. But I think if you talk to them a little bit more you find out that they also look at portions of the analysis, and tie them back to their limited scope performance tests. That what they're seeing there also, you know, rings a bell as well.

And then, you know, if I'm the one that's actually looking at these results from model and simulation, and trying to get some confidence they're working well, I probably would want to know, you know, where the data came from.

A lot of them come from data libraries that have been used and developed in the Department of Energy and the Department of Defense. I'd probably ask questions about how robust is that

data?

Some of it I think we find it turns out to be fairly robust is we look at the PH/PK, which is Probability Hit/Probability Kill, with the battle simulation part of it.

What, it appears that even if I decrease the effectiveness of my protective force, that the likelihood of winning the battle and still killing the adversaries still stays pretty high. And probably a good explanation of that is that there's so much lead flying that some of it's going to hit somebody. So I think that --

And some of the utilities have actually done that analysis. And we have to degrade their protective force very significantly before we see any change in those results.

I think if we look at the part of the data that looks at the detection systems, you know, those are fairly, you know, common detection systems throughout both the whole nuclear complex deemed defense, you know, at NRC regulated facilities.

That if they're installed right, if they're calibrated, if all of that stuff is done properly we could probably have some level of

confidence that the numbers that are associated with those detection systems are probably reasonable.

What I have a tendency to be more concerned about is some of the traversal times, and response times, and things like that. Because really what you're trying to do is make sure that the protective force can actually engage the adversary before they get to the target.

And so the, you want to have a little, understand really the uncertainties in some of those traversal times of the adversaries, and the response times of the protective force. Or, how long does it take them to get through a barrier or through a fence, things like that.

Because that's probably the one area of these modeling and simulation that if you're off, you could significantly impact the results. You know, that's my professional opinion. You know, we, you know, other people may have other opinions. But that appears to be probably the weakest link in the thing, in my opinion.

MEMBER BLEY: Thanks. That helps. But, I'll ask the folks who actually talk about some of these computer based tools. To your

knowledge, do they do much in the way of V&V, QA on the actual code development?

MR. RIVERS: Well, you know, the vendors will put it through all of the, you know, international guidelines for quality code, and all of that.

DOE and DTRA did do some V&V work on multiple codes, two that you'll hear about this afternoon, the AVERT from ARES Security, and SIMAGINE from RinoCorps. In that they will periodically, in fact, they're getting ready to do some of that.

It won't be a complete V&V. But part of the problem is that it's, things constantly change. As the computer technology change, the softwares are constantly being changed. So some of what you have to do is really look at the results.

And do they make sense? Are they consistent? If I make this little change, does it really adversely impact things? Or does it make what I would expect generally?

So, it's not probably the V&V you might expect from a widely used, you know, software program like you have on your cell phones, because of the, you know, billions of people that use them.

You know, this is used by a very limited set. And, you know, you have to be doing V&Vs almost constantly. And the Government can't afford that.

MEMBER BLEY: Okay. Thank you.

MR. RIVERS: Okay. So these are the four general types of tools. If you look at tabletop exercises, it's a method to simulate an adversary attack on a site's existing or proposed physical protection system, similar to a board game.

It analyzes the most common things we look at in security, the detection, the delay, and the response. It also provides insight into a physical protection that can stand alone, or be used in other analysis tools.

You tend to find that a lot of these tools feed information, and receive information from other tools of that type.

Computer simulations, if we look at, you know, how some of them are actually, what they actually do, some of them are pathway analysis that look at how does the adversary actually move through the facility, generates what is the optimal path, or the various paths they might use.

Some are based on the types of scenarios that you might want to actually exercise. And then both of the ones you'll hear about this afternoon have a combat simulation element to it.

So they all have different elements, and they're constructed differently. But these are probably the three most common things that are involved in these computer simulations.

MEMBER CORRADINI: Are these just degrees of the same thing? So, the first one you just kind of wend your way through the maze? And then there's various mazes? And then there's actually stuff happening as you go through the maze?

MR. RIVERS: Right, yes.

MEMBER CORRADINI: Is it just --

MR. RIVERS: Yes. The things will happen. Some of them will have the adversary making decisions based on, you know, what the level of firepower is, how much delay, have I been detected? All of those types of things get factored in.

So, as the computers become much more powerful, you know, the complexity of these simulations has gotten much, much more complex.

And you'll hear a lot more about that this afternoon. So I'm probably not the best person to ask those questions to.

We go to limited scope performance test. This is where we'll have a manual exercise to assess the effectiveness of a portion of the overall physical protection system. And the results can support other VA tools.

So, a lot of times what will happen is, even on the force-on-force exercises they want to figure out how long does it take for somebody to climb over a fence, climb over a wall.

They'll run those exercises independently. And then when they get to the force-on-force exercises, they won't run that part. They'll use the values that came up in the limited scope performance tests.

Also, these limited scope performance tests also validate information that may be found in the modeling and simulation. Or it may feed information that, you know, that provide the data that actually goes into that.

Force-on-force inspection is actually the full scale security exercising, using mock adversary forces. And it does provide essentially

how well a given scenario works. But probably in the end what force-on-force exercise tells you is, does the system work as a whole? Yes.

MEMBER RICCARDELLA: Excuse me. This is my first exposure to any of this kind of stuff. So if my questions are naive --

MR. RIVERS: That's okay.

MEMBER RICCARDELLA: -- please forgive me. These force-on-force drills, are they unannounced? Or does anybody say --

MR. RIVERS: No, there's --

MEMBER RICCARDELLA: -- show up for work Saturday --

MR. RIVERS: No.

MEMBER RICCARDELLA: Friday morning we're going to have a force-on-force drill.

MR. RIVERS: They're very, very complex, and require a lot of planning. So they are not unannounced. Essentially what you end up having to have is, you have, you actually have a real guard force. And then you have a guard force that plays in the game. And then you have an adversary force.

MEMBER RICCARDELLA: Okay.

MR. RIVERS: They're typically

performed in the nighttime hours, because there's less impact then of having plant people involved in the exercise. And usually what will happen is, they'll say, we have a window that sometime in this timeframe the attack will take place.

And so, you have the onsite force that has to be there to guard the facility. And then you have the other ones that are sitting there waiting for the attack to take place, knowing it's going to take place within this two hour window, or whatever. So, very, very complex, very, very complicated. But definitely staged.

MEMBER CORRADINI: So, if you tell us to wait, I'll wait. But to follow-up Pete's question. Is there, are there, if I take it away from the plant is there some importance that it has to be at the plant?

MR. RIVERS: There's a --

MEMBER CORRADINI: Versus if you're not going to involve the guard force that's already there, that you'd have some sort of facility that is more generic?

MR. RIVERS: The facility, this actually has to take place at the plant. Because each plant has a unique set of targets, a uniques

protective posture.

MEMBER CORRADINI: The geometry --

MR. RIVERS: Right.

MEMBER CORRADINI: The geometry matters enough.

MR. RIVERS: Right.

MEMBER CORRADINI: Okay.

MEMBER SKILLMAN: Joe, I'd like to ask this question. Please feel free to say later or no.

MR. RIVERS: Okay.

MEMBER SKILLMAN: it seems to me that, and I've watched these. In the middle of force-on-force you've got your onsite team doing what they're there to do. They're protecting.

Then you have the adversary force. And I've seen these folks. And they are mighty capable. And then there's the responding security force that's responding to the threat.

It's always seemed to me that that is among the most vulnerable times for the unit. Because you got to be careful to figure out who's who. Who's really guarding the chicken coop. Who's in and who's out.

MR. RIVERS: Well, and you have a lot

of controllers. And it's a very, very active time.

MEMBER SKILLMAN: My question is, is that assessed at a level that ensures that the true force guarding is able to do what it needs to do?

MR. RIVERS: I'm not an expert in this area, so I can't really respond to that. But I would believe that that's always the number one issue is protecting the plant. So if something happens that could potentially jeopardize it, the exercise would be halted.

MEMBER BLEY: I think we're getting close to areas that probably ought to be --

MEMBER SKILLMAN: Fair enough.

MEMBER BLEY: -- done later.

MR. RIVERS: And we talked about target sets and safety/security interface. It's an important element of both computer simulations and force-on-force exercises. And it's the minimum combination of equipment which is, if prevented from performing their intended safety function would like likely result in a significant core damage.

So, as I said, these target sets are actually pulled from the PRA cut sets. So, and actually, you've got a large number of these. So

you pretty much have to take a subset of those that make the most sense to actually be evaluated.

And that's actually the end of the presentation. So I'm more than happy to take any additional questions.

MEMBER BLEY: I'm sorry. I just want to throw one comment, and then I'll give it to you, John. The last thing you talked about. I don't know if any of the rest of you remember when the first PRA was done, WASH-1400, the Rasmussen study.

Norm Rasmussen and Saul Levine were asked by people in Congress, and some other places, isn't publishing this study like putting the combination to the safe on the window of the bank vault? And there's been worry about that.

MR. RIVERS: I know.

MEMBER BLEY: I mean, it is the thing you go to to figure out how you would want to do stuff.

MR. RIVERS: But part of what we assume though is that they will have all of that information anyway because of insiders.

MEMBER BLEY: That's true too.

MR. RIVERS: But we have to protect with the understanding that that information is

available.

MEMBER STETKAR: I suspect we'll get -- You know better how this day will unfold. But Joe mentioned right at the end that, you know, there's a large number of cut sets from a typical PRA. And that some winnowing process needs to be used to identify the cut sets that are used, I guess to inform these types of activities.

There's kind of an interesting concept that you don't necessarily look at the dominant cut sets, if you will, from an internal events PRA, because those things are at the top of the pile because of unique attributes of the numbers that are run through the PRA, that are identifying vulnerabilities for a security assessment.

You might need to look down at the bottom of the pile, which is difficult to see, because it might be, because of the numbers that are used in the quantitative analyses there might be combinations of things that could be very, very bad, but are very, very unlikely to occur --

MR. RIVERS: Yes. Yes, I would --

MEMBER STETKAR: -- that you want to look at. So I'm kind of interested to find out how this vulnerability assessment uses those cut sets

from the PRA to kind of inform this process.

MEMBER BLEY: I think you might want to save this.

MEMBER STETKAR: Yes.

MR. RIVERS: What I would do is say this. You may also get some insights when Steve Fogarty talks --

MEMBER STETKAR: Okay.

MR. RIVERS: -- after the break.

MEMBER STETKAR: Okay.

MR. RIVERS: Because Steve has participated on both sides, PRA analyses and VAs. And so, he can help you understand how --

MEMBER STETKAR: I thought you'd said that. You just left yourself open.

MR. RIVERS: That's okay.

MEMBER STETKAR: You have something that says questions, so I wanted to ask.

MR. RIVERS: That's fine. I know how to pass the buck to later speakers. So, not a problem. So, any other questions?

MEMBER BLEY: Joe, thank you very much.

MR. RIVERS: Okay.

MEMBER BLEY: And I guess now we go on to Marc Nichol. Thank you. You can help him find

his -- Oh, after asking everybody to make sure we stay on schedule, I didn't mean to stifle comments. And we're actually 15 minutes ahead of schedule.

MEMBER STETKAR: You're doing well as Archie Bunker.

MEMBER STETKAR: And I could be Edith if you want.

MEMBER BLEY: Marc, please go ahead.

MR. NICHOL: Okay. Thank you for inviting the Nuclear Energy Institute to come and talk with you today. I'd like to discuss the paper that we submitted in November of last year, focusing on consequence based security for small modular reactors and advanced reactors.

We submitted that paper after having put quite a bit of thought into it. If I back up a little bit, and sort of paint the situation, or the stage at the time.

The NRC staff had sent up, I believe it's SECY-11-184, that discussed the conclusion that the current regulatory framework was adequate to license and approve small modular reactors and advanced reactor designs.

And we don't disagree that small modular reactors and advanced reactors could be

licensed under the current regulations and guidance. That's true. But we don't believe that it's the most effective or efficient way to do so.

And so, after putting some thought behind what would be some generic policy issues to be addressed, and how they could be addressed without having design specific information, we came up with the approach that we outlined in the paper. So that's what I'd like to discuss today.

I'll cover three main areas. One is why a consequence based security framework is necessary for small and advanced reactors. I'll discuss the approach that we laid out, and more importantly the policy issues that we framed in that paper. And then discuss the path forward.

MEMBER STETKAR: Go ahead.

MR. NICHOL: Okay.

MEMBER BLEY: That will happen occasionally.

MR. NICHOL: And then --

MEMBER STETKAR: It tends to eventually go away.

MR. NICHOL: Okay. I think we're clear. And then discuss the path forward, and why we believe we need to start today to develop this

framework. I'll start off discussing why small and advanced reactors are different from large reactors.

It's really the reason that we think things can be done more effective and efficiently for these reactors. It's based on a concept that as technologies evolve and advance, we think the regulations should evolve and advance with them.

And so, small and advanced reactors are looking at enhancing safety. That enhanced safety in turn has some enhanced benefits to security. And there's also opportunities, because these are early in their design stage, to incorporate additional enhancements to security, if appropriately incentivized to do so.

So, some of the difference is, they're simplified, they're more simple designs. For example, small modular reactors don't have large piping. Small modular reactors have smaller cores, more inherent and passive safety features.

Small modular reactors are, all the designs currently being discussed are underground, which provide additional benefits. There's a, all of those translate into reduction in potential accident sequences. And so, there's less scenarios

in which accidents could occur.

And also, a slower accident progression, and longer coping time. So even if an accident does occur, then the consequences of such accident would be less, because the accident is slower to progress.

All of those together significantly reduce the risk of radiological release, and offsite consequences. And that's true in the safety area. And that would also translate into security considerations as well.

And as I mentioned, there's also an opportunity to further enhance the security of the designs early on in the process.

So, the paper is recommending that the requirements be a right size for small and advanced reactors. It's looking at having the equivalent level of protection.

MEMBER BROWN: Excuse me. Does that mean reduced?

MR. NICHOL: It could. When we're talking about the security staff there are options in there that, if you were to provide more security base through the design features, the engineered features, that there would be opportunities to

reduce some security staff, yes. And I'll go through that in more detail.

MEMBER BROWN: It just seems to be problematic, that's all. I mean it's --

MR. NICHOL: Yes.

MEMBER BROWN: I understand your point, since we've done, we've had considerable small modular reactor meetings. But the idea that I even have a 300 megawatt plan sitting there with a bunch stuff somehow has some less radiological long term, you know, consequences.

And so as soon as you hear consequence based and right sizing it just seems to me to be, I don't know, problematic. So I just wanted to make sure I understood the thrust of --

MR. NICHOL: Okay, yes. And the approach that's outlined in the paper is really looking at what we're terming security by design. So it's trying to achieve security through the design features, the engineered safety features, and the physical barriers.

And it's an approach that's consistent with the NRC's policy statement on advanced reactors, which is to reduce the reliance on human actions to achieve safety and security.

And so, the premise of the paper is that in order to further encourage security by design there need to be commensurate benefits for the designers and the potential operators.

So, certainly they're going to meet and exceed the current requirements for design features. But there's not much incentive to go beyond, much beyond that, if there's no opportunity for savings.

And there's up front costs to include further enhancements and considerations of security in the design early on. There could be additional up front costs in the construction of facilities that are further enhanced through design features for security.

And there needs to be an incentive to do so. And that would be to be able to capitalize on the benefits of reduced operator, reliance on operator reactions.

MEMBER BROWN: It seems -- I just want to make an observation. I mean, all the security stuff, and I'm not an expert in this, you know. I'm just an electrical guy. I'm someone that feeds comment. I'm not a, hearing some of this for the first time.

But thought, thinking about it is that security, regardless of how you think about it, is really a function of controlling the access to the plant, and those parts of the plant which have consequence, severest consequence results if you get into them.

And the large, large plants, where you have a large facility, a wide barrier, fencing, whatever the barriers are, you have, it's more difficult. The control of access has more things to go through.

Whereas, with a smaller plant arrangement, and if you look at the size of the sites where these have been going they're smaller in many cases, in most cases.

It seems like the easier the access is, or the closer the access, you would seem to have to have an increased physical presence at some sites, in order to minimize the access to the pieces that could give you problems. So I'm just putting that out. And I don't expect a --

MR. NICHOL: Yes.

MEMBER BROWN: -- large coherent answer to that. But it just seems, I don't think the basic assumption going into it is very good.

That's just my thought process.

MR. NICHOL: Well, there's two underlying assumptions in the current requirements that we need to state. And they may not be applicable to small and advanced reactors.

The first assumption is that without a security force to interdict and neutralize, the design basis threat would cause radiological sabotage, or risks that are not acceptable. And that may be true for small and advanced reactors.

The second is that even if the design basis threat were able to cause, was able to cause core damage or sabotage, that that would actually result in offsite consequences that aren't accepted, and that unacceptable. And that may not also be true for small and advanced reactors. So that --

MEMBER BROWN: Are you saying that the consequences may be? You said may not be unacceptable. That means to me they may acceptable. Is that?

MR. NICHOL: Correct. Right.

MEMBER BROWN: So, it's okay to have the stuff spilling outside the boundaries of the site, of the plant facility?

MR. NICHOL: Well, the --

MEMBER BROWN: Just because of the size of the dose --

MR. NICHOL: It may not do that at all.

MEMBER BROWN: -- of the --

MR. NICHOL: So this is one of the central policy issues that need to be addressed. So, one, some designs may be able to achieve a condition where the design basis threat comes in and can't do any damage at all. And so, without considering the activities or human actions of the security force, that's one condition that needs to be addressed.

Another condition that needs to be considered is that if the design basis threat causes say core damage, and there's no offsite release of radiological material, that's another condition that needs to be considered, and determined whether that's acceptable or unacceptable.

The third is if the design basis threat causes damage that results in offsite release, but the offsite release is very minor, much below say part 100 limits, is that acceptable or not acceptable?

So these, we've tried to frame these as policy issues that need to be addressed form small modular reactors. These policy issues didn't necessarily apply to large reactors, because large reactors may not be able to achieve those types of consequence based results.

MEMBER BROWN: It seems to me TMI had no offsite problems at all. And yet, it literally stopped the entire nuclear program of expansion of plants in the country for 30 plus years. So that assumption seems to be not have been born out.

Same thing applies with the Japanese experience. Nobody died, that I'm aware of, yet from radiological consequence. And somebody might. But I'm not aware of it, or at least I personally am not from our discussions.

Yet, that had massive reverberations also when they shut down their entire, virtually their entire nuclear industry since that occurred. And they're just struggling to get it back. So I just look at that statement relative to how we operate. And so anyway, I'll let you go on.

MR. NICHOL: Yes.

MEMBER BROWN: I just wanted to make sure I understood the thought process you all were

going through.

MR. NICHOL: Right. And those are good --

MEMBER BROWN: I'm not saying it's right or wrong.

MR. NICHOL: Yes.

MEMBER BROWN: I'm just asking questions.

MR. NICHOL: And those are --

MEMBER BROWN: That's all.

MR. NICHOL: Those are good considerations. Because I laid out three or four different types of potential consequences. And what's needed is clarity to the applicant on what is the performance standard that needs to be met.

And so it's, that's a wide range. It could be very narrow and conservative, which means that the design basis threat's not capable of any core damage. Or it could be something different from that.

So I think a lot of discussion is needed. We didn't put in our paper a specific answer, or our belief on what the answer should be. Because we wanted the paper to be the starting point for a discussion with the NRC and other

stakeholders.

We want to get everybody's opinion in the process. And we want to get it started early and up front, so we can bring out all these good insights.

MEMBER BROWN: Okay. Well, thank you.

MR. NICHOL: Yes. So the other things is that the NRC requirements, there are performance based requirements that are prescriptive requirements. What we would like to see is a more performance based, and a more technology neutral approach to it.

So I mentioned some of the assumptions that have gone into the regulations, based on the characteristics of large light water reactors that may not be appropriate or true for small and advanced reactors. So those types of considerations.

and I mentioned incentivize reduction and reliance on human actions. I think we have a choice going forward. Do we want to continue the current security paradigm, where there's a heavy reliance on human actions to protect against the design basis threat?

Or do we want future designs to achieve

that more through engineered features, and have less reliance on human actions? I think the NRC policy statements on advanced reactors is clear on that.

And if we do want to reduce reliance on human actions, then I think we need to begin now. Because designs are in the process of being developed. And if we wait too long then these considerations can't be incorporated into the designs. They'd be too far along.

So, I've talked about some of this. So protection by design alone. That's the central policy issue that we framed in our paper. And the question is, if protection of, if protection against the design basis threat can be achieved by the design alone, then what's the appropriate role of the security organization? And what are the performance based requirements for those engineered features?

And we talked a little bit about different types of consequence based results in consideration of the performance of engineered features. And so, that's the question of, which is the right level of performance characteristics that need to be achieved to provide that high level

assurance of adequate protection?

The other is the security organization. So in, if a design were able to protect against the design basis threat by engineered features along, is the actions to detect, assess, interdict and neutralize appropriate? Or are they unnecessary?

We have proposed that if, for security by design the appropriate approach would be detect, assess, and then communicate that threat. Communicate that that threat exists to offsite law enforcement, which would come and support.

So that's consistent with what's been done in other areas. That's consistent with fuel site facilities, with used fuel installations, where the risks of, and the consequences that could be a result of the design basis threat's attack are considered, and deemed that that communique portion is an appropriate response. And that interdict and neutralize is not necessary.

And just to make sure we're all clear, the design basis threat would be the same for advanced and small reactors. We're not proposing that the design has an influence, or would change the characteristics of the design basis threat.

MEMBER BLEY: I feel moved to make a

few comments. In your paper you very often in your talk about security by design. And I think I wish your paper were titled that for several reasons.

I don't think anybody can argue with the idea that we can design in better features to protect either individual targets, or sets that would affect whole processes, that sort of thing. Two areas trouble me. And I know it's a prospective paper. So I appreciate you bringing it and sharing it with us.

The first aspect that troubles me is the title, Consequence Based Physical Security. Once you decouple likelihood from consequence, and I think this consequence based rather than risk based, risk informed, you challenge someone to come up with an unacceptable consequence that would undermine your whole house.

And I've yet to see any systematic approach that involves our reactors, and many other hazards, that can survive on a consequence based approach alone. Because somebody can invent some approach that will make the consequences worse than you thought of.

Once that become very unlikely, we can live with that. But if we have a system that locks

in on consequence based, we have a system that I don't think can be stable and work.

The other piece of this that bothers me is kind of where Charlie was coming from, 300 megawatts isn't tiny. And sets of several hundred megawatt facilities all hooked together on some common systems need to be thought of very carefully in this area.

Your argument that the design basis threat ought to be the same for everybody is one I can understand. But if we design to a design basis threat, and protect against it, we're very vulnerable to something akin to imagine a line.

Somebody will come up with a new threat you haven't thought of. And it may be a very reasonable one. I mentioned I was involved in this Gen 4 project that was looking at perforation resistance of physical security.

And one of the things we hung up on quite a bit was, you know, a single design basis threat might not be the right way to go. You might need a threat space, or a threat set.

And if we're going to try something like you're proposing, I think we need to be very, very careful about what that space of threats might

be. Because it's very easy to game a particular EBT, and build your system to it's in, you know, pretty well invulnerable to that.

And maybe there's a slight modification in the threat for which you're now vulnerable. So I think this whole approach requires a lot of thought and careful consideration.

MR. NICHOL: Okay.

MEMBER SKILLMAN: I'd like to support Charlie's gut instinct. What I'm interpreting from what you're saying, Marc, is that particularly for the SMRs, NIE would think a small guard force or a small security force would be adequate.

And with sufficient design features almost a Mayberry RFD with one policeman who has a .32, and is, on his hip that's empty, and he has one bullet in his pocket. And I certainly don't share that point of view.

I think there are two threats that need to be considered. One is the perceived threat, and the other is the real threat. My own view is the public would have extreme negative reaction to the idea that you could have an SMR that really isn't strongly protected.

But I also have another point of view.

And this came after years of TMI. I remember our security force at the time of the accident was generally men and women, each carrying a revolver, uniformed. And they spent most of their time telling people to go down the road, that they weren't allowed to drive onto the island.

And I watched that security force go from being a small handful of men and women, to being a force that was greater than ops or maintenance. And I understand why those changes came.

But in the middle of that metamorphosis to more and more security, I think what those of us at the plant realized was that the guard force was there, the security force was there to protect us.

Clearly they were there to protect the fuel, the spent fuel pool, and the facility. But at the end of the day we realized they were teammates. And they were there to defend us so we could do our jobs operating that facility.

And it seems that that part of the discussion isn't being clearly communicated. That force does two things. It protects the facility, and the vulnerabilities in the facility. But that force also protects the people who are licensed to

operate that facility.

I watched that happen when Pierce Ne drove through the gate in 1997. And that was the event that brought the industry its security barriers, it's Jersey barriers. I was the EDESD for that Sunday morning.

We were less concerned about the facility, and more concerned about whether that person was a shooter, and whether that person would take out our staff. Let me make that point again. We were concerned whether that person was a shooter, and that shooter was going to take out men and women on our staff.

And I would just offer, if you use that lens to think about what you're proposing here, you may come up with a different point of view. We can talk about protecting pumps, pipes, and heat exchangers all day long. We can talk about protecting buildings.

But that security force protects men and women who are able to drive that plant to a safe shutdown, and to protect it. Those people are important.

MR. NICHOL: Right. And I agree with that.

MEMBER SKILLMAN: Thank you.

MR. NICHOL: I agree with that. And I, hopefully I haven't given the perception that we're advocating for no security force, or even, you know, just a single guard with a side pistol.

There still would be a security organization that needs to perform other functions, like search and seizure, and access checkpoints, and all those things.

There would certainly be people there to guard, and make sure the facility is safe, is secure. And I do agree that protection of the people is important as well.

What, where we're coming from in terms of what would be required by the regulations, stemming from the protection of the radiological material, that's what we're talking about here, in terms of what we think the regulations should say.

I think the plants will go above and beyond that to protect their people. But that's, you know, up to the companies to protect their people. It not necessarily needs to be dictated in the regulations to protect people. So, but I agree it's important.

So, and to go back to the other point,

in terms of the size, and not being small. The definition of small is certainly less than 300. And it's up to the design to actually be able to demonstrate they can achieve these performance criteria that would need to be established.

Not all small reactors would be able to do that. Would a 300 megawatt reactor be able to do that? Maybe, maybe not. But a lot of the designs are much smaller than that. So some are even down in the 20 to 50 megawatt size. So they're much smaller.

What, to translate security by design into other terms. One performance based criteria would be the elimination of target sets. So if you had no target sets to begin with, what's the correct security posture to protect the plant at that point? That's what we're asking.

And the regulations are very prescriptive that you need to have ten armed security guards with the sole duty of responding to the design basis threat. Are those ten guards still necessary if there are no target sets? That would be one extreme.

And then the other would be, if you did have target sets, maybe it's a target set with a

large number of pieces of equipment that are protected very well with physical barriers, that the design basis threat does not have the resources and capabilities to actually do harm and damage that target set.

So those are the considerations. And of course, the designs have to prove that they can achieve those design criteria.

It's, we're not proposing that all small and advanced reactors get a pass on this just because they call themselves so. They would actually have to demonstrate that to the NRC, that they could achieve whatever performance standard that's set.

And looking at the major policy issues, we talked quite a bit about the security organization response, that the performance standard. I highlight there unreasonable risk to the public. And so that's a major question. What is reasonable, unreasonable risk to the public?

I appreciate your comment about if we focus only on the consequence, we're ignoring the probability side of the risk equation. And I think that's true.

In our paper we didn't attempt to

explore the use of PRA or probability on the, or the likelihood of the types of attacks that would occur. We took it very much as Joe talked about earlier, as a probability of one, or a conditional, if this occurs, what happens next?

If that were to change in the future, I think it could certainly be applicable in this area. But we didn't see a trending to change that approach, at this time anyway.

But there may be other uses of PRA that aren't in place today. So Joe also talked about the --

MEMBER BLEY: I'm sorry. Even if you don't put in a probability of attack, when you do the kind of analyses that Joe was talking about, you get out a probability distribution of consequences. So they're not, even in a conditional analysis, probability is part of the answer.

MR. NICHOL: Right, right. Yes. And we'd certainly like to talk about how that could be introduced. We don't have a strong position on it right now. We'd like that conversation to occur though.

And other uses of the PRA. So, it's

used to identify the target sets. That's based on significant core damage, or spent fuel sabotage. If that's still the performance metric for small and advanced reactors, then maybe the use of PRA may not be much different.

But if the performance metric were instead the possibility of releasing radiological material from the site, or a dose based standard offsite, then perhaps the use of PRA could be expanded.

And then there are other areas of the requirements that, depending on how the major policy issue is answered, may need to be looked at. So, what are the requirements for the use of firearms, or the armaments that are needed at the site? What about the use of deadly force, and the applicability of the NRC's policy on that.

And is there a need for force-on-force exercises? Or do they, could they be something different than what's done today? And all that depends on how the major policy issues are addressed.

I think what you may be getting a sense of is that our paper posed more questions than answers. And certainly that was the intent of the

paper. We wanted it to be a point of discussion with the staff and other stakeholders.

We recognize very much, as you pointed out, that the public will have their own perceptions of what we're proposing here. And will have their own perspectives and questions to be answered. And we want to make sure that they're engaged in this process as well.

That's why we're, that's why we believe that the discussion needs to start now. I know that the NRC SECY, part of the justification on why the current regulations are adequate is because there's a process for alternative measures and exemption requests.

And certainly we could go that route. I don't think that that's the most efficient or clear. If we draw the parallel, there's many parallels with what we're proposing on security, and what's being done in the emergency preparedness space for small and advanced reactors, in terms of the basis and the consequence based approach that we're trying to achieve.

The NRC Commissioners approved to go forward with rulemaking with that. And part of the decision, or part of the basis for approving moving

forward on rulemaking with that was that doing that now, rather than waiting for exemption requests was, provided one more clarity to the applicants, more regulatory stability.

But it also provided an early opportunity for stakeholder involvement. And I think that's what's needed on this topic as well. In terms of the clarity to the application, business decisions are being made.

And decisions on the design are being made today. So, if a designer is looking at how they can enhance this for safety and security, the framework itself has an influence on what they consider, and what they try to achieve with that design.

The current framework is very prescriptive in what's needed for the security organization. I don't believe there's incentive to go very far in enhancing the design for security.

If there were opportunities to gain benefits on the security organization side, then there may be more incentives to further enhance the design. And I think that's something that we should pursue.

MEMBER CORRADINI: So, can I ask a

question at this point? So I think I see your, where you sit. So, how much have the current owner/operators looked at this, given that they are on the front lines of doing it now, compared to what might be done?

MR. NICHOL: They, so security is one of three of the major business, major regulatory issues that are going into the business decisions.

MEMBER CORRADINI: No. But I'm asking something different.

MR. NICHOL: Yes.

MEMBER CORRADINI: Maybe I asked it -- So, if I went to Exelon, which is running 25 plants, and they have a security plan that meets current regulations, and they look at this, what would their reaction be?

MR. NICHOL: In respect to their operating --

MEMBER CORRADINI: In other words, do they agree with the general feeling that improved security by design, whatever Dennis called it. I like the way he said it.

MEMBER BLEY: And it was their words.

MEMBER CORRADINI: Would essentially, they would at least see the attributes that you're

after. My only point is that it seems to me, where I would go are the people that actually have to make this happen now.

MR. NICHOL: Yes, yes. Yes, the --

MEMBER CORRADINI: And their reaction to it. Kind of what is being asked.

MR. NICHOL: Yes. The owner/operators had input into the NEI paper. And they see that as a, you know, a good way to move forward as well. So, now, we don't, we didn't propose that this be applied to the operating reactors. Not that it couldn't. But we didn't propose it to be.

One, because it may require extensive modifications to the plant, which would be cost prohibitive. And the other is, we're looking at this as a going forward. But --

MEMBER CORRADINI: Right. But the reason I asked the question the way I did is I'm kind of reflecting on Charlie's reaction and Dick's reaction, as a Navy reaction and a former operator's reaction to it.

So I'm trying to get a feeling for what the reaction was of those that are actually now having to make this work, given current regulations. That's what I guess I'm getting at.

MR. NICHOL: Yes, yes.

MEMBER CORRADINI: Okay. Yes, and I, if I wasn't clear before. The reaction was positive. So, the regulatory framework in this area can be developed without the design details.

Certainly design information helps give confidence. But a lot of what we're talking about are the more general high level policy questions that we discussed earlier in establishing the performance based criteria, which doesn't necessarily need design details.

We have seen, from what we know about small modular reactor designs, and advanced reactor designs, we do believe that they are capable of this. Not all of them will meet whatever performance standard is established, or would be established. But some certainly could.

Talked to, starting now would also develop a regulatory basis that would support near term exemptions and rulemaking, if those are necessary. Certainly we're not going to be timely enough for near term SMR applications. Probably can be timely enough for advanced reactor applications.

But nonetheless, developing the

regulatory basis would support that. And I already talked about how it's, about similar concepts with what's being done in EP and advanced reactors.

So, given the time, just to reiterate. So, we think the existing requirements aren't appropriate for small advanced reactors, a consequence based approach, or even something that incorporates more of the risk insights could be, is needed, and should start now.

Our paper's just a point for starting that discussion. And we look forward to that discussion. What we would hope to see is a meeting in the relatively near term with NRC staff, to discuss the paper, their considerations or questions, get other stakeholder input into that.

We hope that the Commission would like to move forward on this, and would make a decision to do so in this year, and establish a regulatory basis next year that, if needed, would support exemptions that we're making. Thank you.

MEMBER BLEY: Marc, thank you very much. Any comments from members of the committee? Some good food for thought. And we appreciate you coming --

MR. NICHOL: Thank you.

MEMBER BLEY: -- and joining us. We're going to take a break at this time. Try to be back by about 10:25 a.m., and we'll start up again. Thank you.

(Whereupon, the above-entitled matter went off the record at 10:11 a.m. and resumed at 10:30 a.m.)

MEMBER BLEY: This meeting is almost back to order. And we're going to move forward with the presentation by Steve Fogarty of ARES Corporation. On the Role of Modeling and Simulation in Risk-Informed Security Decision Making.

And this is kind of a break from the overview and philosophy that we've done so far and we're going to get into some of what the meat of today's session is about. At this point I'll turn it over to Steve. Thank you for joining us.

MR. FOGARTY: Yes, thanks for the opportunity. I appreciate it, Dennis.

So what I want to talk about today, a little bit of the history, if you will. Because this is as much a perspective, as anything, on modeling and simulation and its role in risk-informing security.

So back in the mid '90's, when I was at PLG, I had an opportunity to apply some PRA technics to DoD weapon systems. And specifically, that involved taking some deterministic components and probabilistic components and combining them together into what the time was a pretty novel application of PRA. But it was still very much accident focused.

So DoD, in an effort to understand their security risks, took that and funded an effort, which I lead, starting with RND all the way through to commercialization of a software tool set. And then later we implemented that tool set at DoD facilities, nuclear facilities DOE facilities and commercial nuclear power facilities more recently.

So then about a year ago I left the vendor community and returned to being a risk practitioner. But in the intervening time, and since that time, there's still some unanswered questions.

I did sort of, with these unanswered question, in and around how best to risk-inform security using some of these methods and tools. So that's what I want to talk about.

So before I talk about how this is done generally, and this is a very general treatment of modeling and simulation. No tool specific, anything.

I want to talk about why we might do it. So that being the benefits of modeling and simulation for security.

So first of all, to get at that, there's these figures for merit that you'll hear. I call these here listed on the bullet there, meaning the system effectiveness metric, defense-in-depth and critical system elements that you get at maybe through a sensitivity analysis as sort of primary figures of merit.

There are many other statistics that you can get at through these processes. It's a data rich process so you're going to get a lot of ability to do that. And understand the program strengths and weaknesses, if you will, through those metrics.

The ability to convey visual information, I think, is pretty unique and uniquely impactful in our ability to do risk communication to leadership. So I consider that to be a significant benefit of these tools. And methods.

The ability to discovery and identify emergent behaviors sort of manifest itself through these unique, and maybe new vulnerabilities, that hadn't been identified earlier. Or an ability to characterize an emergent threat.

So there's a litany of secondary benefits as well. First off, the safety security interface and enabling that. I'll try and touch on that where I can.

Just sort of warning you, I have a pretty expansive definition of risk. I like to include frequency, consequence, all components of it in my, whether or not I can quantify all the pieces as a secondary effort. But I'm going to focus on the compatibility, where it exists, and contrasts. And some cases, with safety, throughout here.

I think it can be applied in various phases of the design. We just heard a talk on SMRs, as one application, when I've got a paper design and can't very well do an OFF. Exercise against that.

So tools like this really provide a unique, I think benefit.

One of the things that's maybe often

overlooked is these tools, although complex and whatnot, the data input is done in a very natural way for those that build these models.

I can talk to a security professional about the time for a responder to get from one post to a response location, where they may be in be interdict and are up, neutralize the adversary. And they have access to that timeline, okay. They already test to that.

If I start talking in maybe more abstract terms, especially with our security professionals, security organizations, such as there are today, about probability of interruption, it's just a little more abstract for them, okay?

And then lastly, the bullets there on their safety benefits. Obviously to over live exercise. I'm not suggesting that we get real live exercises, but more about, in cases where there's an option.

And for example, I am a first responder, I might be able to, I don't get in that facility very often, I can use some of these models that are secondary benefits. Get in through an orient myself, to these facilities, through these models.

All right, so how we might go about it and specifically, you know, how do we do it successfully in implementing this? So first thing is a terminology, and I'll hit more on terminology in a minute.

The term there, PSMS, physical security modeling and simulation, is just the way I characterize, if you will, the security application of risk, or PRA. Okay?

Here. So you we'll see that throughout. The statement there is just one in a paper that I wrote on this subject and more of a thesis statement.

But what I want to focus on are the two items there. To be successful I think there's an effort that needs to be put forth to get the data in such a way that we can build these models. Okay? And I'll talk a little bit about what's required there.

And then also the methods. A little on the methods that are used generally in the tools that are there, and by the analysis.

And then secondarily, how we use them and what's the context for using these to risk-inform a decision?

So you'll see there's been a few papers and presentations I have given. There was one at the RIC last month, in this area.

Okay, so on creating input. So regardless of the tool I'd like of think that this is, this is how I see it anyway, are the inputs necessarily to build these models. Three tasks, if you will.

So we have to characterize the facility into something that I term as a security virtual environment. So think, starting with, there on the chart there, virtual environment.

This is our facility, as we recognize it, but in the computer. Right? So this is our 2-3D model. All the terrain elevation, whatnot.

And so that's our representation, our virtual environment, if you will, the facility, and we're going to lay over top of that the security that goes with it.

So fundament to security. And you've seen already, I think in Joe River's presentation, detection, delay and response. Our fundamental concepts, not only required, but in that order, to protect a facility. Of any kind.

So here we're just laying down those

things that exist. Where detectors are, where the delay systems exist on that. And collectively we create this security virtual environment. Okay?

So that's Step 1 in the process. Step 2 then is, well how do the components perform? These are the speeds that are, and whatnot, say over a barrier using certain equipment, say by an adversary. The performance of our weapon systems that if they're utilized, by either in the hands of the security force or the adversary.

And there's just a lot of data that goes into that. But we have to understand the performance piece, or what I call PDL there. Performance data library.

And then lastly we've talked a lot already, I think there's been some discussion on the threat. And this isn't the DBT so much, as the implementation locally in the DBT, into the scenarios that we're going to run to understand the securities. So those are the three inputs.

And now I want to maybe talk, a little bit, of the departure, but directly, hopefully in line with the meeting, some of my thoughts on the safety security interface, through the terminology that we commonly use.

So for, at least for this presentation, I'd to think of that first column there, PSMS column, as the security application of PRA or risk. And the PSA columns as the safety side. Okay?

Meaning, I'm just trying to use it as a way to compare some terminology.

So you've got the security virtual environment, that I just talked about in the last chart. And we really don't, I can tell, we really don't have something there on the PSA. Not that we can't create our system models of the facility but we don't use them, at least as a general approach in PSAs, to actually quantify the risk. Okay? That's abstracted.

And so if you go to the next row there, the fault tree/event tree logic, for example, is our abstraction and represents the failure logic for the power plant. But there is analogy to that. And I'll talk about this on the next chart or two.

But for now we'll call it the adversary/traversal graph, if you will. That is if you think of the adversary as your agent to failure, maybe that's your comparison to safety there. And mathematically there's also a correlation, I mean direct relationship, a tree

just being a subset of a graph structure.

So the next piece of comparison, the PDL that I called on the prior chart, performance data library, is directly comparable to the terminology we use in safety for failure rate databases and whatnot.

Target sets and, and it should, probably here in this case, say we either begin with minimal cutsets or just say cutsets. But there's a relationship.

We've already heard about it. And unfortunately I'm not going to be the expert, I don't think, on experience in building those target sets from cutsets, but generally you've got to account for more than just the minimal sets, right?

You got to look at co-location of equipment when looking at cutsets for failure. What's co-located? Maybe a piece of equipment is in a less protected location.

Those all go into selecting from the family of cutsets. Which ones then build up the target sets. So it's a special information combined with the cutsets, from the PSA.

MEMBER STETKAR: Steve, you said you're probably not the person to talk about that, are we

going to here today from anybody who is?

PARTICIPANT: No.

MEMBER STETKAR: I think that's -- okay, thanks.

MR. FOGARTY: Okay, so then on the threat scenarios and initiating event piece, I think there's, I think we all understand we need a driver for this analysis to go forward. So those are, in that way, they're the same.

But it's also a clear and significant difference between the random components of failure in the initiating events and the actions of an intentional adversary. Our adaptive adversary.

So it's bolded there and I'll treat it on a subsequent slide.

So here's my, back to my comment, that expansive definition of risk, if you will. Whether it's conditional or not, I put that frequency in my formulation because I believe it's important to recognize it. And in the consequences as well.

But what I really want to drill down to here, because this is where PSMS is focused, is the likelihood estimate. Okay?

Conditional likelihood given an attack that the adversary is successful, okay? So I'm

going to touch on those. So both of those bolded items I'm going to touch on, here in the next charter.

MEMBER CORRADINI: So can I just say it back to you so I understand?

So you do assign something to the --

MR. FOGARTY: The frequency?

MEMBER CORRADINI: Oh, I was going to say, I guess the threat scenario is what you call it. The initiating event, you do assign something?

MR. FOGARTY: Well the typical approach, whether it's guaranteed or not, right, you assign something. So yes, if you're saying it's guaranteed or once per whatever unit of time you want to look at --

MEMBER CORRADINI: I understand. I just wanted to make sure I understood what you're saying.

MR. FOGARTY: Right. And really the purpose of this here is not to get into how we might do better at that, but I believe it's important to recognize --

MEMBER CORRADINI: But your point is, it's included in the calculations?

MR. FOGARTY: Yes.

MEMBER CORRADINI: Okay.

MR. FOGARTY: I think so. All right, so the adaptive adversary -- go ahead.

(Off microphone comment.)

MEMBER BROWN: Sorry about that. Go back to the Slide 5.

MR. FOGARTY: Sure.

MEMBER BROWN: Your line that says, adversary agent traversal graph. And it says, the adversary graph can be determined, automatically, from the SVE, the security environment, virtual environment, while the FT/ET logic is developed by a risk analysis.

I guess it puzzles me that, yes, you may know what the pathways are, but you've got a, this is not like a normal cut set in a PRA where you've blacksmith technology. You know, pipe breaks, water goes out, valve opens, blah, blah. You can predict what goes in some circumstance. Most circumstances.

These are humans. And they don't necessarily conform to a path. They get smart as they go through.

How do you factor in, at least the experience I've got from people, like seals guy

that you know, says that they go in and they never know what they're going to encounter. If they have a path and they, most often never use the path. They alternate, they improvise and they have to as they go through.

How can you say or how do you say you have any validity to the predictions when now, when you've got a human involved in making decisions and changing what they may do, even as they start initially?

MR. FOGARTY: Well I guess first of all, I'm going to agree with you --

MEMBER BROWN: Oh.

MR. FOGARTY: -- that if you don't do that, then you've got a problem. And it is sort of fundamental and foundational to the difference between safety and security that we address that.

MEMBER BROWN: Yes.

MR. FOGARTY: And it's actually on my next two charts.

MEMBER BROWN: Oh, okay. I just --

(Simultaneously speaking.)

MEMBER BROWN: -- automatically and --

MR. FOGARTY: No, and I did that intentionally to identify it as it sort of

distinct.

MEMBER BROWN: Okay.

MEMBER BLEY: I think I'm right. I think this afternoon you'll see some actual simulations where we'll actually see that happen.

MEMBER BROWN: That's fine. I just wanted to make, I hadn't heard that in all the previous discussions and this was the first time I saw the line item that implied. It's automatically determined from the environment that's the traverse path and I suspect that they won't use the traverse path that they initially planned on. More than likely.

MR. FOGARTY: Yes, I can agree with that. I'm not -- I'd be interested in your comments on whether you think the approaches that are out there are valid, but definitely there's an effort to --

MEMBER BROWN: Okay. No. Okay, just wanted to make sure I understood. Thank you.

MEMBER RICCARDELLA: Charlie, I'd just like to say I object to the term blacksmith technology.

(Laughter.)

MEMBER BROWN: On a comparable basis,

okay, pipes and iron and steel and valves and wire and insulation have been around since, well the iron and steel --

MEMBER BLEY: Thanks, Mr. Brown, I think we got that.

MEMBER BROWN: What? And the insulation and the electricity have been around for 150 years. So the basics, fundamentals, are as they are. But the new technology is far more sophisticated. So it is blacksmith technology. So we'll have to agree to disagree.

MEMBER BLEY: Steve, please go ahead.

MEMBER BROWN: Okay, thank you. Got to have some humor here.

MR. FOGARTY: So the first statement there at the top is really, how do we got out these? I want to identify the steps or what will start to introduce this term pathways, a given threat could use to defeat the system, okay?

And we're going to start out here, I'm going to try to generalize in just four steps, the way these tools compute that likelihood estimate that you saw on the prior chart. And we'll see how well they do.

So the security virtual environment

that I mentioned, okay, it needs to be broken down into some component parts or data structure. One of those is termed navigational mesh.

I don't know how well you can see it, but in the notional figure there, the little triangular pieces that are in there, and breakup the model that's there on the right, are what you might term that navigational mesh.

So we're going to breakdown that data structure, into this navigational mesh. Historically, if you look back, back to even to the mid to late '70's, Sandia created ways to do this using a much more even closer analog to PSAs.

If you take, they're called adversary sequence diagrams, you take an event tree and you like rotate it 90 degrees, it looks kind of like that. So there's a lot of history there.

There's just be more automation, and that's maybe the navigation mesh is where that comes in. So I have to break into pieces first, okay.

MEMBER RICCARDELLA: I'm sorry, you talked about triangular pieces. I don't --

MR. FOGARTY: Yes, I don't know if you can see them well on there. Yes, they're probably

a little hard to see in the figure. I don't know if you've got a hard copy. It may be a little easier to see in the hard copy, but --

MEMBER CORRADINI: Can you point?

MR. FOGARTY: Sure.

MEMBER BROWN: There's some quadrilaterals in there.

MR. FOGARTY: Yes. So the triangular pieces here and here, everything is broken into, in some form, into triangular pieces of concave pieces. And it's really just a mesh --

MEMBER STETKAR: Steve, make sure you're close to the, you can use the mouse --

MR. FOGARTY: Oh, sorry.

MEMBER STETKAR: -- make sure you kept close to the --

MEMBER BROWN: No, you can use the screen right here.

MR. FOGARTY: Oh, there we go.

MEMBER STETKAR: Yes, there you go.

MR. FOGARTY: There we go. Now I can see --

MEMBER STETKAR: And you can see.

MR. FOGARTY: Now I can see it too. I don't have to look behind me.

MEMBER BROWN: No you don't, you can look right up here.

MR. FOGARTY: Yes, be trained on this. So here's one of the triangles, for example. It goes from here and then there's another one here.

Okay, so what we're really doing is we're trying to say if you go from a start point to an endpoint, I have to traverse through these paths. And I do so by this, breaking this side into little pieces. If you will, triangular pieces in one way or another.

So that tree structure that I mentioned, that is created historically using those sequence diagrams, adversary sequence diagrams, is sort of automated in the sense that the edges of the triangle become maybe nodes, if you will, in the tree structure. Okay?

So I'm basically creating this tree structure, or graph as we call it mathematically, somewhat in an automated sense. By my ability to break the site down into pieces. Nodes and edges if you will, overall.

MEMBER RICCARDELLA: Okay, now that you pointed them out I can see the triangles.

MR. FOGARTY: Can you see it better?

Okay.

MEMBER RICCARDELLA: On the --

MR. FOGARTY: Sorry, I should have done a better job on the figure there. So now I have this and I want to find the path. You can see one of the paths here.

So for any given structure, if you think of entries, fault trees having split fractions or weights, as we'll call them here, we need a weight along the penalty, or cost if you will, to get from one place or another. Okay?

MEMBER CORRADINI: Just so I got it, when I entry a point, I have three choices, you just give me a weight as to, at least a dynamic weight, as to where I might go?

MR. FOGARTY: Yes. And we'll talk about the weights on the next chart. But let's for minute just say, if I have the weights and I have the graph, I can actually solve for the minimum cost to target. Okay? Okay.

And there's a lot to that. But I want to get to the point that was brought up early, on Step 3 here.

So I'm going to virtually, now I've got this model, if you will, and I've got an attack

plan, if you will, for the adversary. Meaning he's going to look at this most vulnerable condition and understand how we perform under this attack like this.

That virtual attack, or simulation, some would say combat simulation. But I like to be expansive and we need to simulation all actions, if you will. Including the combat component of it.

They perceive down the path as planned. But they need and ability to adapt to conditions, especially the stochastic nature of things, as things evolve. Okay?

So they need both an initial plan to sort of look at the greatest vulnerability and try to attack along that and be able to adapt as they go.

And then simply speaking, that likelihood estimate, is very simply the number of times the adversary was successful over the number of times we simulated his attack. And that's how we get at that estimate. Sort of an objective probability estimate, if you will.

Okay, so that's just the steps. Now I'll talk about the weight, if you will. How this, because it gets to the behavior part of this, for a

minute.

So try to classify the way these behaviors work. There are, in my mind, a couple of ways, nowadays, that this is done.

The first classification I want to use is what I call task-based models, okay? So adversaries are going along and they are through interactions with our subject matter experts. They have a defined set of mission tasks they need to accomplish. From that start location to the end being the target sets, if you will. So they have this defined.

But between them, think of it maybe as the route between the tasks they have to do. If they're breaching one barrier and then another, they have a route between those two, they can adapt.

So they have an adaptation, okay, in a task-based model. They do adapt. They just don't do it in the same way that this other one is, which is the preference-based models.

And those preference-based models look more, if you will, globally at vulnerability for the facilities. Finding the best route and task. Not just the route to get there. And they do it on

these preferences.

Their preference being, how much do I want to minimize detection. How much do I value that versus minimizing delay, versus minimizing being neutralized by the protective force.

In this case, the modeling is very global and expansive, but it requires more data. And is more computationally expensive.

So back to the application quickly, for a minute. DOE will, for example, will use these task-based models. They use them on a fairly regular basis at their facilities. Their nuclear facilities.

And they do so because they fully believe they already understand what some of these tasks are. And they feel like they already have a very good handle on their vulnerabilities, okay?

So, it doesn't mean they don't use the preference-based models, but they gravitate a lot to task-based models because of that. It's also the only one that's in NUREG-7145 on security risk assessment. At least as I see it mentioned there.

Preference-based models are very good at searching for new vulnerabilities. So if you had a new design, you're trying to evaluate it for

the security system, they kind of tend to be good at that.

They can also do the whole picture and the whole security effectiveness performance measure. But that's just a strength up there.

By way of example, there's a preference-based model that's kind of listed on the, now that I know how to use the mouse here, that's listed on the chart here. And to give you more, just an example how some of this stuff may work.

So this is a phase one. So early on they attack, the adversary minimizes their chance of being detected. They transition at some point to a delay focused minimizing their time to target, if you will.

And then they transition at the next threshold to a balance between, and this is probably they're in some combat kind of simulation or combat kind of environment, and they're realizing, not that they don't care about, you know, they're certainly willing to die for their end goal maybe, but they understand that they're neutralized, they can't achieve their objective either. So they have to balance their ability to

be neutralized with the time target.

So that's just one example that's referenced there.

Okay, so one of the other key factors in doing this is, what uncertainties are we facing? And this is by no means an exhausted list or even a list of all the things we ought to treat. But these are things that I, from experience, believe are not just important, but maybe commonly overlooked uncertainties, when doing this.

So decision making. This decision making focused on deployment of officers, shift tactical commanders, such as they are.

A lot of our sites, they all have this concept, even if there's preassigned response locations. If an adversary makes it through, maybe outer layers of security, there's always a concept of flex to redeploy forces on the fly.

And all I'm recognizing is that we need to account for that. And I'm not trying to exhausted interview every one of these guys, but appreciate the uncertainty and the effect on performance.

The second one is, failure of the security system. Not due to the adversary failure,

but failure due to the latent failure, much like PSA kind of thing.

So I'm going to give an example if that because I think it's kind of telling and there's some lessons in there, on the next chart. And that's why it's bolded.

The others I think you can kind of get. Operating modes, target sets for example. If I'm in a detention in the reactor head I'm probably in a more vulnerable condition than I am in full power operations, for example.

So these are just things that I believe need to be looked at. And I thought, if I could, I'd give you an example of one. To kind of tell a little bit of a story.

So this is the event. I'm guessing many of you at least heard about this at some level. But back in 2012, we had three protestors at a DOE facility that penetrated the exterior layers of the security system. Okay?

And I guess I want to talk about, is there anything to learn from this? And we better learn something, in my opinion.

And I think there's some stuff specific to PSMS. Or Mod Sim for security that can be

learned as well.

So I separated it in the way I see it. The equipment and human performance side into two separate pieces.

So first of all, I'm not here to say that the material in the facility was ever at direct risk, but I don't think it can be argued that the system functioned as designed. I think it clearly did not.

So it's a question of, where was the failures? So first of all, there on the equipment side, there was a critical assessment camera at this facility.

So as the protestors made their way through the outer layers, they couldn't slue the camera to assess. So detection requires sensing and assessment. We didn't have assessment and we really didn't have detection, fully.

And they had a lot of history of high nuisance alarm alerts at the facility. Just exasperates the problem.

Next was human performance. On that side, our primary assessment patrol didn't respond fast enough.

It wasn't just slow response, it was

outside of the timeline that they had for that individual, in total, including uncertainty to respond, okay? So that is another failure.

And then the last is, the alarm station operator didn't declare a high priority soon enough, if you will, as expected. Okay, so those are just two areas.

And then I state the statement, well okay, so PSMS, it reinforces the benefit of that for this. But that's not the whole story.

PSMS was actually used at this facility. And so you might say, well great, so why didn't it find this problem?

This gets down to the fielded system and the analyzed system. The system as fielded, had these issues in it. The system as analyzed, assumed these things were functional, okay.

There's nothing I'm telling you probably that you've not seen before in other situations. But I think it's a critical part of the connectivity between this and the fielded systems, if you will.

So we were basically analyzing an idealized system and we weren't going to find anything. And in fact maybe made it, us, maybe a

little more confident than we should have been because we had these results.

All right, so back to risk, down to risk informing decisions here. I want to talk a little bit about how that process might work.

And I'm going to do it in the framework of Reg Guide 1.174. I just think it's a good framework for risk informing decisions and I don't, but I'm going to use terminology from security.

So defining a proposed change is how we start the process. So this doesn't necessarily mean I'm looking at it in the, I'm trying to be expansive in the way I look at decisions too.

It could be an NRC decision that gets advanced through a 5054 popup change like you've heard about already today. Or it could just be any decision. I'm sort of advocating for where security fits into the decision process, regardless of who the decision maker is.

So first off, if we can use it in early in the process, we know where we're sensitive, where system is sensitive, we can optimize a good, we can come up with a good change. Is one area.

But regardless of what kind of change we have, we need to perform some form of analysis,

okay?

And I guess I'm just mentioning, and Joe Rivers mentioned earlier, it's really a combined effort, right? It's PSMS and Mod Sim and it's limited in full scope performance testing, it's force on force, tabletops, all that kind of thing. So it's a full picture of performing analysis, okay.

But once we have that analysis, the other aspect of the decision process is, okay, if we're going to implement that and maybe post implement, how are we going to monitor it? How are we going to ensure that we were actually right and the assumptions were protected that we, as we field them? So we have to come up with a way to define a monitoring program.

So what I've done there, in the figure below, is really just to speak to things that I think are, can kind of tell somebody how to put a model like this together.

It is one of the biggest problems in modeling and simulation, is not having a scale for how big your model needs to be to support the decision at hand. And you end up spending a lot of resources building these models sometimes. And

sometimes in the wrong area.

So these are just areas for physical security that I think are important to look at.

So the system layers. So, I don't know, generally we have the owner controlled area outside the plant, we have the protected area and then maybe the vital area inside that. So just generally, those layers is what I'm talking about.

As I get through those layers of the security system, the more of them I get through, I would qualitatively expect higher levels of detail in my analysis to support that change. Because it's affecting multiple layers of the security system.

Similarly, on the other axis there, if the critical elements in my system, that previously identified were critical to the performance, I need to protect those. More of those impacted, more detail expected.

And lastly, thinking of those design areas are fundamental concepts to security, detection, delay and response. If I'm going to affect my ability to detect, delay and respond, yes, I'm going to need more details.

This is not anything quantitative here,

but just an idea to help those that build these models, kind of look at how much detail to put into them. In their analysis and also in their monitoring, I believe it could apply equally well to both of those.

So lastly I need to document these changes. So I'm going to document them in two forms, right?

I need a decision document that the decision maker is going to sue to understand their performance and what decision is being advanced. And it's supported by technically basis documents, depending on the analysis that was done, okay?

I'll come back to that because I think it's kind of a critical difference between safety and security.

So as I wrap here, the next two charts as I wrap up, before I conclude, I guess I wanted to point out who's doing this currently and what their nuclear experience is with this.

And I want to point out what DOE does, as I see it. Having worked with them, sort of when this was emerging, if you will, with them and their interest in Mod Sim.

So they have more of what I call a hub-

and-spoke configuration in their use of these tools. They have a center with DTRA, Defense Threat Detection Agency, is just one of them.

But as a good example, that the services and bases and units in the field can access to get Mod Sim done for them. But they don't typically have that capability in the field, okay. With trained expertise, okay.

They also, so I would say use it intermittently, as needed. However, you want to describe that, on the DoD side, for physical security.

And then lastly, it was mentioned, verification and validation. There's a whole topic for discussion on how that's done.

I'd be happy to talk to that, but DoD, for example, has done formal tool verification validation and accreditation activities. Of course you have to verify the implementation of the tools and whatnot. But they've done some of that.

On the DOE side, they have more organic, as I said, their risk assessment teams. They're trained up in the fundamentals of this, they've been leading the community, I think in this area, in terms of implementation of some of these

tools.

They'll typically apply more than one tool set in-house, and do sort of this best to breed kind of decision making on which tool to use at a particular time.

Problem there is that can be pretty cost, I don't know if it's cost prohibited, but certainly costly, depending on who you are. At least getting them spun-up and trained-up and kept current.

I mentioned their existing policy can be difficult when adopting new approaches. I think that's sort of expected.

They have a regulatory framework for using these, they require them, DoD does not. Okay, so that's kind of a big difference.

So they're going to have polices. And I will say you'll hear from Sam Callahan, I think, this afternoon. He's really the expert in this area and has been working hard for policy change, including a new design basis threat that they're about to come out with in DOE.

So my last sort of summary here talking about, I guess I want to focus on the decision maker's expectations when it comes to this. In

terms of moving forward if we're going to use these, what are the decision maker's expectations?

With respect to, and let's just maybe focus it maybe on an NRC for example. What are the reviewers of submittals that come in and when they're reviewing a change to a design, what are their expectations with respect to modeling uncertainties, treatment of those? Do they need to be treated, how to treat, qualitative, quantitative, sensitivity analysis and that kind of thing.

Okay, so that one thing I think that's important to move forward with, we need to understand those expectations.

One reason why, right, is, well for quality purposes, but also those that implement these, licensees or whatnot, if they don't understand what their deliverable is, that is to say what there is expected of them, they're less likely to dip their toe into doing this, if it's seen as a benefit. And the benefits of the whole process get advanced the more that participate. I think.

So I think that's one of the reasons.

Referenceable performance data is on

there. Mainly to focus, not on the data itself or data quality, but the fact that we really need to keep an eye on, in my opinion, on how referenceable that data is.

But that gets back to the decision makers expectations. What are they going to except?

I mean we sometimes will see it say, subject matter expert, as the whole reference behind where that data came from. And I'm not out to say that expert elicitation and subject matter experts aren't ideal candidates in some cases for certain types of data, because we can't get at them another way.

But I would say that's an insufficient generally and insufficient answer, without a basis for their logic. And it gets us in a situation, at least, that we might reuse it in an inappropriate way.

Peer review. What are their expectations, prior to decision makers seeing the decision document, what peer review has been done on this work?

So, and then the last pieces here, there isn't a common data library. So think

generic failure rate data basis. There isn't such a thing, okay.

Currently there's a lot of data. Okay. DOE and DoD have shared a lot of data through these initial analyses with NRC. And I think that's a very powerful thing.

But there hasn't been anything capture with respect to having a common library that can be used. And I think that goes a little to quality, in my opinion.

There's a limited quantitative experience in this community. Doing quantitative analysis in general and documenting it.

That's just a sub-bullet there, it's just a suggestion that I think the PRA analyst community might be able to, at the licensee merit, help them understand what a technical basis document really typically looks like kind of thing.

And then I think, because there's just out, the applications today, in my opinion, can be very tool-centric and not focused on the decisions. I mentioned the 3D models.

You can overdo that, right? You can go into a situation where the tool is really good at building these cool looking models. And they're

great. But you can overdo that. And it takes a lot of resource into doing that.

And when you do that, that resource gets expended, there's no going back and recovering it. And it wasn't necessary to support the decision in the end, probably. So that throttling of that I think is largely just to do with the fact that there hasn't been a lot of tools implemented.

And then this last one is a little more policy level, which isn't my strength, I'm an analyst. But it's just my feeling on the subject.

I think as we do more, there's going to be more of a tension, a natural tendency to compare safety and security risks. If we quantify risks and security, we have quantified risks and safety, we at least need to understand that people are going to want to put them down next to each other and say, wait, why is this one so different than that or are they comparable.

And I think there needs to be an effort to at least explain it, if not drive it all the way down to normalizing some of the assumptions that exist, where it makes sense, between them. So that's what I wanted to cover and take questions.

MEMBER BLEY: Steve, thank you very

much. Anything from the Members? Charlie, just a short one, we're running out of time. No soliloquies, Charlie.

MEMBER BROWN: Okay, Slide 10. You talked about levels, systems layers impacted. And that you had less detail in the outer layers and more detail as you walked your way into the inner layers. At least that's the way I read in critical systems elements type thing.

And I'm just trying to think, why in the world would I want my out layer to be breached in the first place? I mean if you look at the classic defense setups that you do in almost all installations, you build one heck of an outer wall. And you don't want to have to be scurrying around inside the inner walls, inside those, to try to stop a threat.

And so to me that would imply that you would want to apply more detail to the ability of an adversary to break through that outer wall first.

I mean the kings in the old days didn't build castles because they didn't want to have to fight it in the villages.

MR. FOGARTY: Yes.

MEMBER BROWN: And so it just seemed to be counterintuitive to me.

MR. FOGARTY: Yes, I wasn't, it's probably just a clarity issue on my part. I wasn't trying to suggest that there wasn't detail in the outer layers of the security, but that the entirety and breath of the analysis that's performed, needs to expand if the adversary, if the change I'm making affects my perimeter fence, like you just said, or my perimeter, as well as my vital area inside the plant.

Okay, so for example, if I have response forces that respond to both locations, right, I've now affected the inner layers of the security system and the outer layers simultaneously.

So I'm suggesting that the breath of my analysis needs to be, it needs to be broader and detailed in such a way to address that. I'm not saying that we don't need security at the perimeter by any means.

MEMBER BLEY: I think we're going to have to stop on that at this point.

MR. FOGARTY: That's fine.

MEMBER BLEY: Steve, thanks very much.

MR. FOGARTY: Yes.

MEMBER BLEY: And again, thanks for joining us. Our next speaker won't be in the room with us, but he'll be on the phone. We have to get the phone line open, which I think you'll have to do.

MR. BUNN: The phone line is open. I'm here.

MEMBER BLEY: Oh, you're here. Oh, very good. If will give us just a minute, we'll get your slides up.

MR. BUNN: Okay.

MEMBER BLEY: Yes, if can speak a little softer or back away just a little bit it will work better. It's coming in very loud.

MR. BUNN: Okay. How's that, is that better?

MEMBER BLEY: That's perfect.

MR. BUNN: Okay.

MEMBER BLEY: Our next speaker, who was just speaking, is Professor Matt Bunn of Harvard Kennedy School of Business, Government.

We've had an introduction and an overview this morning of kind of why we're doing all of this, what's going on and where it can be

useful. And a little bit of what some of the tools are beginning to look like.

And I think Professor Bunn will maybe give us some things to ponder about where we need to be careful as we go forward. I thank you very much for joining us this morning, Matt, and at this point we'll turn it over to you.

I have to say we do have to end promptly at noon because there is another meeting that's challenging us as well. So I'll turn it over to you at this time and some of the members may ask you questions as we go along.

MR. BUNN: Okay, that's fine. So thank you very much for the opportunity. I apologize for not being able to be there. I wish I was there.

It was in the 20's when I was last outside. We've got two or three inches of snow on the ground here.

MEMBER BLEY: Matt, if I can interrupt you, if you can back your sound off just a little more.

MR. BUNN: Okay.

MEMBER BLEY: It's too loud here.

MR. BUNN: How's that?

MEMBER BLEY: That's better.

MR. BUNN: So I apologize both for not being there and for, unfortunately, I was in another meeting and wasn't able to take part in the earlier discussion. So it's at least conceivably I may be repeating some things that have already been said.

Next slide please. So I would argue that computer tools for vulnerability assessment are extremely helpful. This is the computer tools as what the staff asked me to mainly talk about. I'll talk about another point toward the end of the talk.

If they're properly developed, then you've had a lot of discussion this morning about the strengths and weaknesses of where we are, so far, on these tools.

They can give you higher fidelity in simulating possible adversary scenarios then just doing, for example, a tabletop exercise.

They can allow you to look at different security options more easily. Which may help you identify cheaper ones or more efficient ones to accomplish the same objectives.

They can help the regulators try to confirm if somebody's asking for an exemption and a

change in what would normally be required. They can help you confirm that, yes, that will actually achieve the objective reasonably well.

They can help give you greater easy in looking at a new adversary scenario that somebody just thought of. And so that helps you have more complete coverage of possible vulnerabilities.

And they can also help you look at what if we did include something else in the DBT or what if there was an adversary that went beyond what's in our DBT right now?

How much would it cost to have an effective system against that, modify its threat or how much can our existing system do to deal with that modified threat? So they can help you model things like that.

Next slide please. But at the same time, it's very important to understand the limits. Nothing is perfect.

And in particular, there's the fundamental issue of, garbage in, garbage out. Models are only as good as the assumptions that go into them.

So I have this famous quote, "all models are wrong, some are useful." And my variant

of that is also that some can be dangerous. Because people tend to believe the output of a computer model.

There's this sort of feeling, oh, it got printed out by a computer, it's got to be true. And I think often we get a little bit deluded by thinking that the real world looks more like our model than it actually does.

So I would say the models are very useful for identifying factors that need to be addressed and approaches for dealing with them. But they're not likely to be very good at giving us an absolute estimate of risk.

Particularly in security where we don't really know what the probabilities of various adversary actions might be. And there are large uncertainties and complexities.

So I'm going to talk about five different particular complexities. One, the overall modeling of complex systems. The complexity of the system itself and the difficulty of modeling it.

You're limited by just the user of the models ability to think of all the defeat strategies adversaries might think of.

There are human and organizational factors that are more difficult to model than the technical factors in the system.

The insider threats are more difficult and the cyber threats make things difficult.

Next slide please. So there are a number of key assumptions that even the best vulnerability assessment tools, they're sort of baked in to the idea of these tools.

One is that the technological elements will perform according to the estimates that are built into the model. Another is that the human parts will perform according to the estimates built into the model.

Another is that the adversary capabilities and tactics will be within what's imagined in the design basis threat.

And finally, the adversaries won't use any strategies we haven't thought of. And that's, you know, of course the number of strategies the adversaries might come up with is pretty broad so we need to think of defenses that will cover a wide range of possibilities.

But still, there may be some defeat strategy that gets at a vulnerability we haven't

noticed or thought about. So any of those assumptions can turn out to be wrong.

Next slide please. So let me talk about these that I mentioned in turn. So one is the difficulty in modeling complex systems.

When a system is complex and you have somewhat uncertain system interactions, when you pull on one side it may cause something to happen someplace else in the system that you weren't expecting. So there's emergent behavior.

And this is a situation where the interactions among the elements, and especially the how the human and organizational elements react to changes in the technical elements, how they react to just the passage of time going by as complacency builds up and so on, is really not well understood. Apologies for the misspelling of understood there. I was doing this quickly yesterday.

So the 2012 incident at Y-12 gives you a good example. They had just installed a new intrusion detection system called ARGUS, that was intended to improve security. But with the installation they had, which may not have been exactly correct, it was leading to many unexpected false alarms. About ten times as many false alarms

as previously.

So normally you'd check out the false alarms with cameras, but the cameras had been broken for months and nobody had bothered, yet, to fix them. And so the guards were getting sent out to check out the false alarms, but if there's ten times as many false alarms, at a certain point you get sick of it.

So these protestors went through four layers of fencing, three of them alarmed. Set off countless alarms, were at the very wall of the building with thousands of bombs worth of highly Uranium, spent a substantial period there singing protest songs, pounding on the building with sledgehammers and were finally accosted by a single guard.

There were very heavily armed guards inside the building who heard the pounding and thought, huh, must be construction, even though we haven't been told there is going to be any construction and even though it's before dawn, guess I won't bother to check.

So there was a pretty profound breakdown in security culture. But if you're just on a vulnerability assessment computer model, you

would have seen all this good equipment and intrusion detection and so on and you wouldn't have realized that those problems were going to come up.

Next slide please. So a second complexity is that it's just hard to imagine all the things the adversary might do. And the tools are only as good as the people who use them.

And so the personal solution to that is to get people with our creative hacker kind of mentality to use these tools and think of potential adversary tactics.

One of my colleagues, Roger Johnston, has a saying. He says, any real system has an infinite number of potential vulnerabilities. Most of which will never be discovered by either the good guys or the bad guys.

And he says, we think that because every time our team looks at something we looked at before, we find new vulnerabilities we didn't notice before. Every time somebody else looks at something we looked at before, they find new vulnerabilities we didn't see before. Every time we look at a system that somebody else already looked at, we find vulnerabilities they didn't find and so on.

So I think one, one thing is, I think it would be very important to establish red teams that are incentivized. Not only assigned to, but reward for finding vulnerabilities. And of course proposing fixes to them.

Next slide please. So this is a fundamental one that gets back to the Y-12 case that I mentioned. Which is, that it's difficult to model how human and organizational behavior is going to change over the years, and even decades, that these systems are operating and in play.

You have to remember that for the average nuclear guard, there will never be a real event in his entire career. So every alarm he ever responds to in his whole like will either be a false alarm or a test.

And so trying to avoid complacency in that situation is actually very difficult. So that complacency in human behavior ends up affecting the various assumptions made about how well the humans in the system do their job.

This is particularly an issue for various aspects of the insider threat. And the degree to which people are willing to report behaviors that might suggest that there is an

insider problem.

My colleagues Scott Sagan and I, at Stanford University, have put out a little pamphlet called A Worsts Practices Guide to Dealing with Insider Threats, where we have a number of lessons from real incidents in the past.

Not only in the nuclear industry but in other context. About the difficulties that organizations have in dealing with the insider threat. Which I'll talk about more in a moment.

But this whole question of, how does the organization and the human factor, factor in to the performance of the overall system, is not well modeled in a lot of these computer tools so far.

Next slide please.

MEMBER BLEY: Hey, Matt?

MR. BUNN: Yes.

MEMBER BLEY: Excuse me. This is Dennis Bley. Can you make that guide you just talked about available to us?

MR. BUNN: Absolutely.

MEMBER BLEY: Yes, I think --

MR. BUNN: I'd be happy to --

MEMBER BLEY: I'd personally be interested in it. It sounds pretty good.

MR. BUNN: I will drop a link to the staff. And I should mention, just as advertising, that we are, we've done a more elaborate version with other authors going into cases in more detail. And also a lot of interesting data on what Jihadis have looked at in this broad category.

MEMBER BLEY: Okay.

MR. BUNN: That will be coming out as a book from Cornell University of Press later this year.

MEMBER BLEY: Oh, good, we'll try to keep track of that and --

MR. BUNN: All right. So I will certainly send a link to the staff for the Worst Practices Guide that's already out.

MEMBER BLEY: Okay, thanks very much. And I just wanted to back up to your previous slide since I interrupted you. And just mention one thing, in pretty much agreement with you.

One thing we found in doing analyses, more for safety than in this area, but it works the same in both, is just the mind shift, I think, of instead of trying to figure out what somebody else will do, saying, I really know the system inside and out, how would I attack it for developing

scenarios really makes a difference and helps.

MR. BUNN: Right. Absolutely. And so I think having that kind of red team sort of assigned to think that way, is quite important.

And that's one thing actually that tabletop exercises are good for. Because you can get a bunch of staff people together, at a site, to just brainstorm about things like that.

All right, so I wanted to talk about Slide 8. The one that says security culture matters. So this is just a demonstration of the point.

I love this picture because this is a propped open security door at a Russian site that had been upgraded with U.S. assistance. And what's great about this photo is it's propped open on the day that the general accounting office is there to take a picture of it being propped open. Which means that the people at the site really didn't get the concept that it was a bad thing that it was propped open.

So security culture can make a big difference on your system. And I can talk about that at lengths, if people are interested.

Next slide please. So this gets back

to the insider point I was making a moment ago. That those threats are more difficult to model.

A lot of the computer tools are really much better on the outsider threat. They're traditional methods based on sort of the detection probability as the outsiders go through various layers of the system, the task time that it takes them to get from one layer to another and then to do the things they need to do to either carry out a theft or conduct a sabotage, the response for survival time and so on.

All of that is more complicated and tricky when you're talking about an insider who's inside the system for months and years at a time. And you may detect things, but you may not realize that what you've detected is something you need to deeply worry about.

One of the things that's been most remarkable to me, in our work on insiders, is the redness of the red flags that people will ignore. So the guy who almost certainly carried out the anthrax attacks in 2011, for example, Bruce Ivan, had written an email to his own staff complaining about his own dangerous paranoia and speculating about ending up in the newspaper under a headline,

mad scientist in control of deadly germs. And nobody reported that.

That was, by the way, one piece of many, many things that if anybody had really been reporting properly, would have led to that incident not occurring. In any case.

So insiders also aren't deeply familiar with the security system and its weaknesses. Or they may be.

Some of them may be the people who designs the security system. And they have a lot of opportunities for social engineering. For convincing other staff to do seemingly harmless things that facilitates a plot.

You see that in amazing detail in the case of the escape from the Clinton Correctional Facility this past year. Where the inmates really succeeded in social engineering with a lot of, with a number of the guards. In addition to the woman who was actually in a romance with one of the inmates. Or sort of in a romance.

And insiders may recruit other insiders. And very few of our DBTs include a multiple insider scenario. But if you look at major thefts in the non-nuclear world, multiple

insiders are at least as common as alone insiders.

Next slide please.

MEMBER BLEY: I want to interrupt you for another time, Matt.

MR. BUNN: Okay.

MEMBER BLEY: In the area of risk assessment, I've often found that the more even antidotal stories one can find, it really helps when you're doing modeling to keep your thinking very broad. Are there good sources in this area for the kinds of stories you just went through?

Are you going to have these in your book or can you send us to some other sources?

MR. BUNN: So I think that is a very important point. I have been advocating for years, so far unsuccessfully, that the U.S. Government ought to put such a thing together. And in particular, that we ought to create a shared global database of incidents and lessons-learned.

You know, in the safety space, if you're a U.S. Nuclear Power Reactor, as you know, and you have some kind of near-miss incident, there's a root causes analysis, lessons-learned that get sent to INPO. INPO does trend analysis based on what's happening in other reactors, that

may be similar.

Those lessons-learned get distributed to the other reactors. INPO even inspects to see how well you're implementing the lessons-learned.

None of that exists in the security world. And I think there are restraints created by security issues, but I think there's a lot that could be done.

If you look in the cyber security world, there is a lot of this sort of data compilation that gets done.

There's a group at Carnegie Mellon, for example, that collects anatomized data so that companies are willing to hit it over on insider cyber cases in many different industries. And they have a database of over 300 particular incidents that you can go through and learn from these different incidents.

And it's a big enough database now that they can do statistics about, well, how many insiders have this characteristic and that characteristic and so on.

One thing I would point you to is a very nice piece, which again, I can send the link to the staff, that was done in Sandia National Labs

a couple years ago called the Perfect Heist.

Which goes through, oh, 15 or so major sort of multi-million dollar non-nuclear threats from garden facilities in recent years and just looks in detail at what was the security arrangement, how was the security arrangement defeated, what kinds of tactics and capabilities did the adversaries have. I think that's the kind of thing that we definitely need.

I'll just give you an example of, in 2003, there was a court case in Russia that revealed that a business man from Nizhny, Novgorod had been offering $750,000 for stolen weapon grade plutonium for sale to a foreign client. And at that time in Russia, that was about a century of the average person's salary.

And he made contact with people who lived in one of the closed nuclear cities in Russia, who promised to steal plutonium for him. Fortunately for the world, the people he made contact with were scam artists who tried to pass off a canister full of mercury on him.

But I have yet to meet a Russian security manager who was aware of that case. And it seems to me if, people are offering $750,000 for

stolen weapon grade plutonium, your security managers ought to be aware of that.

So sorry to go off on a rant on that subject, but --

MEMBER BLEY: I'm sorry, there was some chuckles here thinking, I hope he's well -- he's the right guy. Thanks, we'd appreciate that.

Is the Carnegie Mellon data publically available or is there a contact there that --

MR. BUNN: Well, it's certainly the case that NRC could get access to it. I don't believe it's available to the public.

There is a book that they've published based on it. A guy named Randall Trzeciak is one of the key people there, but I can send relevant contact info to the staff.

MEMBER BLEY: We would appreciate that a lot. Thanks, Matt.

MR. BUNN: Okay. All right, so I'm now on Slide 10, cyber threats.

So these, as you know, I'm sure you've talked about those in the Panel before, they're very difficult to model in part because the adversary capabilities are mutating and evolving at fairly frightening speed.

And also the vulnerabilities that we have in cyber, you know, the zero day is called that because you're vulnerable when somebody discovers that on that zero day. And so you don't necessarily know you have that vulnerability until all of a sudden it's discovered.

And then there's the interactions between cyber threats and physical threats.

I gave a similar talk at a workshop here in Boston, that the staff organized with the Institute for Nuclear Materials Management. And the key thing that the audience objected to in my talk was when I asserted that of course we're all thinking about the interaction between the physical attacks and cyber-attacks. And various people in the audience said, no, nobody is really thinking about that effectively yet.

And people at Pacific Northwest said, but we are, but we're in the early stages. So I think there's a lot more work on thinking about exactly how could what different levels of adversary use cyber to interfere with the physical security systems and contribute to their physical assault. Whether it's a sabotage or a theft scenario.

A lot of the physical security systems are becoming more and more and more digital. And therefore potentially vulnerable.

Next slide please. So I would say we should use these computer tools, but we should be aware of their limitations.

Department of Energy and Department of Defense, as you've probably been hearing this morning, have used these kinds of tools for a long time. To good effect.

I do think that overall, the use of these tools has greatly contributed to improved security and improved efficiency of security. Although nobody will claim, in either Department of Defense or Department of Energy, that efficiency of security is where it needs to be, yet.

We're spending, especially in the Department of Energy, an amazing amount of money on security these days.

As you may or may not know, the annual Department of Energy budget for security, which isn't all nuclear facilities but is mostly nuclear facilities, is in the range of $1.8 billion. So that's a lot of money for not a huge number of facilities that the Department of Energy has.

But we do need to avoid putting more reliance than they deserve on these models. As I said, they're no better than the assumptions.

I think when you're thinking about, should we reduce a requirement or make an exemption based on the results of a model, you need to put in some expert judgment as to how important that change is. As well as only relying on the results of a model.

So it should be informed by the models, but not entirely based on the models just as in safety.

And I think as you shift towards more performance based approaches, the realistic testing, including a really good force-on-force program, is going to be critically important, I think. To make sure that the security systems really do perform as well as we think they do, in the face of adversaries who are intelligent in trying to think of ways to beat them.

Next slide please. So I just wanted to talk for a moment about material attractiveness. I think it absolutely does make sense, as the staff is proposing, to have less security for material that would be much harder to make into a nuclear

bomb.

But I think the current staff proposal, in my view, goes much too far. And I know the staff doesn't agree with me and we've been back and forth about this on quite a number of times now.

The current staff proposal says, if you got less than ten percent by weight Plutonium-239 or Uranium-235, you can drastically reduce security to the point that the security plan can be based on the adversaries steal the material and then local law enforcement is in hot pursuit.

I just think that goes way too far. We have very modest reason for confidence that hot pursuit will always work. NRC doesn't get to regulate the local law enforcement and the hot pursuit because it's local law enforcement. It's not the licensee.

I think there's been many past U.S. Government studies, including NRC studies, that have concluded that it's not a good idea to rely so much on dilution. So this is a change from past NRC policy. And it would lead to us having the weakest rules in the world for security for that kind of material.

Which I think is the wrong direction

for the United States to be leading. And I've put up there a link to a more detailed public comment that I made on that subject.

So that's the end of the slides I wanted to do. So I am totally open for questions. And I apologize for going on so long.

MEMBER BLEY: No, that was wonderful. Thanks, Matt, we really appreciate your time. I'd ask if any of the members have any questions for Matt at this time?

I think we're running too close to lunch, Matt. We're out of questions. But we really appreciate your presentation and the links you've given us to new information. And we will make use of that in the future, and we hope to see you one of these days.

MR. BUNN: Okay. I hope to be there one of these days.

MEMBER BLEY: Thank you. At this time, I think we're going to go off the record and end this public meeting. Oh, but I have to look for comments first.

Can we get the regular phone line open so the public can make comments? And I will ask at this time, is there anybody in the room who would

like to make a comment on today's session?

We'll wait a few minutes to get some indication that the phone lines open.

MR. BUNN: I'm going to stay on just in case somebody has a question for me.

MEMBER BLEY: Okay.

PARTICIPANT: The lines open.

MEMBER BLEY: I've been told the line is open. Is there anybody on the public line who would like to make a comment at this time? If so, please identify yourself and make your comment.

MR. LEWIS: My name is Marvin Lewis. And I don't know if it's a question, I don't know if it's a comment.

MEMBER BLEY: Oh, okay. Well go ahead, Marvin. Thank you for joining us.

MR. LEWIS: Okay. I'm just wondering, if these defenses, if this security isn't setup for an atomic bomb, nuclear bomb, that was designed back in the '40's?

Right now, this 76-year-old name Sam Kohen, K-O-H-E-N, who worked for the Clinton Administration and says we have the ability now to make a 25 pound bomb with very different characteristics then the new bombs nowadays.

And I'm not saying it's right, he's right, I'm not saying he's wrong. But I respectfully respect, suggest you look at 615, 7, by Christopher Ruddy, R-U-D-D-Y, he's a reporter.

And he says, this bomb inventor is speaking the truth. And he's in the Tribune Review. I don't know where they are.

MEMBER BLEY: Okay. Well, we would --

MR. LEWIS: But I'd really like to raise a question. Are these security measures for a time in the '40's and not a time in this century? Thank you.

MEMBER BLEY: Marvin, thank you very much. I've been advised to say that the Nuclear Regulatory Commission, the Advisory Committee, don't have anything to do directly with weapons and that's true.

But thanks, Marvin, for you comment. We will make use.

Is anybody else on the line who would like to make a comment? All right, at this time we'll close the public phone line. And I go around the table and ask the Members to make any comments they'd like to.

And today's meeting is an information

brief, essentially, but any thoughts you have are welcome. Why don't we start with you, Pete?

MEMBER RICCARDELLA: No comment.

MEMBER SKILLMAN: No comments, thank you.

MEMBER STETKAR: Nothing at all. I'm interested, learning.

MEMBER BROWN: Fascinating briefs. Thank you.

MEMBER CORRADINI: Okay. Well, at this time I would like to thank the members of the public for their comments and I'd like to thank all of our speakers for a very informative day. We've learned a lot.

I'd particularly like to thank Joe Rivers and his staff for helping us put this together and for organizing those IM/MM workshops, which were really helpful and really opened our eyes a bit to lead to this session today.

And I want to thank Christian Lui, because she's really put this whole thing together today and made it work. There's been a lot of coordination to get the various groups here.

For the Members, we're going to break now and we'll have a PMP meeting at noon. The

session back this afternoon is closed.

And part of it will be absolutely closed with no electronics here. No cell phones, no computer, no watches that talk, none of that. So when you come back, you may as well not bring any of that back here with you.

At this time, we'll go off the record for today and we will end this meeting. It's adjourned. We'll start up with the other one at 1:00.

(Whereupon, the above-entitled matter went off the record at 11:47 a.m.)

1

2

Overview of the Physical Security Regulatory Framework, Vulnerability Assessment Approach and Safety/Security Interface

Joe Rivers

Office of Nuclear Security and Incident Response

April 6, 2016

U.S.NR

United States Nuclear Regulatory Comm

Protecting People and the Environ

Outline

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Physical Security Regulatory Framework
- Safety/Security Interface
- Risk-Informing Security
- Vulnerability Analysis

NRC's Power Reactor Security Program

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- **Purpose:** To provide HIGH assurance of adequate protection to prevent significant core damage and spent fuel sabotage.

- **Objective:** To ensure security programs are established such that licensees can protect against adversaries up to and including attributes described by the Design Basis Threat (DBT) in order to prevent radiological sabotage.

- **Process:** Develop NRC licensing and inspection programs, as well as, industry initiatives that implement and verify the level of protection described.

Licensing

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- For Operating Nuclear Power Reactors;
  - 10 CFR 50 and 73 Security Regulations apply
  - Formalized process to make changes
- For New Reactors:
  - 10 CFR 52 and 73 Security Regulations apply
  - Final Safety Analysis Report (FSAR) must describe the engineered physical security programs
  - Implement security requirements before fuel is allowed inside the protected area
- The NRC utilizes NUREG-0800, “Standard Review Plan,” and various Regulatory Guides to conduct security plan reviews and approvals

Security Plans

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Regulatory Basis:
  - Provide physical protection against the design basis threat (DBT) of radiological sabotage
  - Establish and maintain a physical protection system and security organization
  - Establish and maintain, at all times, properly trained, qualified and equipped personnel required to interdict and neutralize threats
- General requirements for the content of each security plan are found in 10 CFR 73.55(c) and 10 CFR 73.54
- Required Security Plans:
  - Safeguards Contingency Plan
  - Training and Qualification Plan
  - Physical Security Plan
  - Cyber Security Plan

Inspection Program

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Process: The commercial nuclear power reactor inspection activities for physical protection programs include:
  - Baseline Inspections, including Force-on-Force Inspections
  - Special Inspections

Safety/Security Interface

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Requirement codified in Title 10 CFR 73.58 “Safety/security interface requirements for nuclear power reactors”
- Applies to operating nuclear power reactors
- Requires a pre-assessment and management of all planned and emergent activities involving changes to plant configurations, facility conditions, and/or security programs
- Communicate potential conflicts to appropriate personnel and take necessary actions to maintain safety and security in accordance with NRC requirements and license conditions

Safety/Security Interface

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Security uses the cut sets from the PRAs to inform the target sets used in vulnerability assessments
- Security vulnerabilities and associated consequences are needed by safety organizations to inform safety programs
- Need to understand the relationship between safety and security risk

Safety/Security Interface

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Need to evaluate impacts on each discipline as changes in plant configuration/operations are planned
- Need to understand how information from each discipline better informs the other discipline

Risk-Informing Security

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Numerous workshops over the past six years
  - Sandia Workshop – 2010
  - INMM Stone Mountain Workshop - 2014
  - INMM Reducing Risk Workshop - March 2015
  - INMM/ANS Sun Valley Workshop - April 2015
  - INMM Boston Workshop - September 2015

Risk-Informing Security Activities for NPPs

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Use of modelling and simulation tools
- Safety/Security risk
- Cyber Security
- IAEA Coordinated Research Project on Nuclear Security Assessment Models

Industry Initiatives

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Submission of security plan changes supported by modelling and simulation
- Consequence-based approach for SMR security regulations

Vulnerability Analysis (VA)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- A systematic, performance-based process that is used to evaluate the ability of a physical security system to meet performance requirements

VA Tools

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Types of Simulations
  - Tabletop analysis
  - Computer simulations
  - Limited scope performance tests (LSPT)
  - Force-on-force exercises

Tabletop Exercise

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

A method to simulate an adversary attack on a site's existing or proposed physical protection system (PPS), similar to a board game

- Analyzes PPS elements:
  - Detection, delay, response
- Provides insight into a PPS that can stand alone or be used in other analysis tools

Computer Simulations

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Pathway analysis
- Scenario Analysis
- Combat simulation

Limited Scope Performance Tests

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- A manual exercise to assess the effectiveness of a portion of the overall physical protection system
- Results can support other VA tools

Force-on-Force

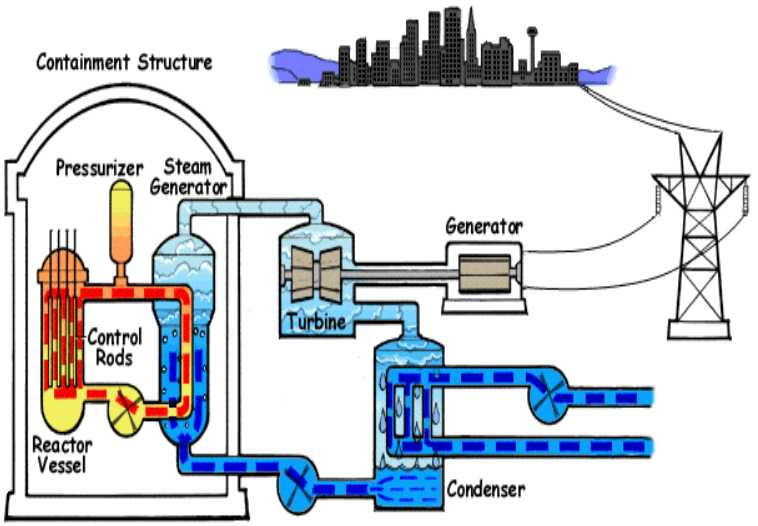
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Full-scale security exercise, using mock adversary forces

Target Sets

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Important element of computer simulations and force-on-force exercises
- Minimum combination of equipment, which if prevented from performing their intended safety function would likely result in significant core damage (e.g., non-incipient, non-localized fuel melting, and/or core destruction) or a loss of coolant and exposure of spent fuel



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Questions?

Consequence Based Security for Small and Advanced Reactors

Generic policy issues and industry's proposed approach

April 6, 2016

Meeting of the

Advisory Committee on Reactor Safeguards,
Subcommittee on Reliability and PRA

Areas of Discussion

- Need for consequence-based security
- Industry proposed approach
- Path forward

Small and advanced reactors differ from current designs

- Simplified designs (e.g., no large piping)
- Reduction in potential accident sequences
- Slower accident progression/longer coping times
- Significantly reduced risk of radiological release and offsite consequences
- Opportunity to incorporate security early in design

NRC requirements need to be right-sized for small and advanced reactors

- Protection of public health and safety equivalent to existing reactors
- Portions of current requirements unnecessarily burdensome for SMRs and ARs
- Should be technology-neutral and consequence-oriented
- Incentivize designs to reduce reliance on human actions

Industry Proposed Approach

Security Element	Existing Framework	Options for Small and Advanced Reactors
Protection by design-alone	Not contemplated	Performance-based
Engineered features	Prescriptive physical barriers	Enhanced safety and security features
Security Organization	Prescriptive (e.g., detect, assess, interdict and neutralize)	Graded based on ability of design alone to protect against radiological sabotage
Design Basis Threat	Independent of design	

Major Policy Issues to be Addressed

Topical Area	NRC Policy Decision Needed
Security Organization Response	Detect, assess and communicate is appropriate if design basis threat cannot cause unreasonable risk to public.
Performance standard for "unreasonable risk to public"	Should be based on potential for off-site consequences
Use of Probabilistic Risk Assessment	Expand role of PRA (e.g., risk informed assessment of off-site dose consequences)
Others (e.g., firearms, use of deadly force, FOF exercises)	To be addressed depending on resolution of other policy issues

Need to start developing framework now

- Security enhancements need to be incorporated early in the design process
- Potential owner/operator business decisions need to be made well in advance of submitting applications
- Can be developed without design details
- Clarity on regulatory basis will support near term exemptions and longer term rulemaking
- Concepts for consequence-based security parallel basis for planned rulemaking for emergency preparedness
- Consistent with NRC Advanced Reactor Policy Statement

Conclusions and Path Forward

- Existing requirements are not appropriate for small and advanced reactors
- A consequence-based approach is needed, and development should begin now
- NEI paper is starting point for discussion
- Proposed next steps
  - Meet with NRC to discuss steps to develop details
  - Commission decision to move forward in 2016
  - Regulatory basis in 2017
  - Near-term exemptions and future rulemaking, if necessary

The Role of Modeling and Simulation in Risk Informed Security Decision Making

ARES CORPORATION

TRANSFORMING CHALLENGE INTO SUCCESS

www.arescorporation.com

Advisory Committee on Reactor Safeguards
Reliability and PRA Subcommittee

April 2016

Steve Fogarty, VP Special Projects

Benefits of Modeling and Simulation for Security

- The primary benefit is a clearer understanding of the security programs' strengths & weaknesses.
  - Measures of system performance such as System Effectiveness (Pe), Defense-in-Depth, and identification of Critical System Elements (CSEs)
  - Conveying "visual information" to leaders on all aspects of the site security posture (i.e., successful risk communication)
  - Ability to capture emergent behaviors such as previously unidentified vulnerabilities as well as emerging threats (e.g., UAS)
- Secondary benefits:
  - Compatibility with existing PSA processes particularly in the area of risk-informed decision making (i.e., enables a strong safety-security interface).
  - Can be applied prior to implementing a design change at an existing facility as well as in new facility design (e.g., SMRs)
  - Model construction and population is done in a "natural" way for the security professional
  - Virtual environment provides safety benefits over live exercises
  - 3D models for virtual tabletop exercises and walkthroughs

Successful PSMS Implementation

*"When operated within their design specifications, Physical Security Modeling and Simulation (PSMS) tools have progressed to a point that they can be counted on to produce a high-quality measurement of the facility's security posture and risk profile."**

Successful tool implementation requires a focus on:

1. **Transforming the current data and facility knowledge into the input needed for PSMS analysis.**
   - Addressed in recent papers and in presentations on *Facility Characterization, PSMS Applications, Model Robustness, VV&A, Risk Drivers*

2. **Providing a context for how the PSMS analysis results will fit into existing decision processes, regulatory requirements, and security design requirements of the organization.**
   - Addressed in a recent paper and a RIC 2016 presentation regarding current industry challenges with balancing analysis scope and expected quality

*Fogarty, S. P., "The Role of Modeling and Simulation in Risk-Informed Decision Making", Proceedings of the 56th Annual Meeting of the Institute of Nuclear Materials Management, July 2015.

Creating the Input for PSMS

PSMS Requires Completion of the Following Three Tasks:

1. Characterize the Facility Into a Security Virtual Environment

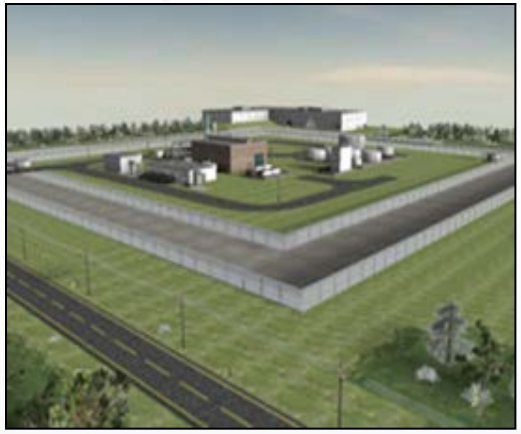
Virtual Environment
- Infrastructure
- SSCs
- Elevation / Terrain

Detection Systems
- Cameras
- BMS
- Vibration Sensor

Delay Systems
- Perimeter Fencing
- Vehicle Barriers
- Doors

Response Force
- Posting/Patrol
- Response Locations
- Vehicles and Tools

Security Virtual Environment



2. Develop the Performance Data Library for the Physical Protection System

Performance Data Library
- Detection Probabilities
- Defeat Times for Barriers
- Speeds Over Barriers and Terrain
- Weapon Hit/Kill Probability

3. Characterize the Threat into a Set of Threat Scenarios

Threat Characterization
- Threat Structure (i.e., teams)
- Threat Size
- Starting Locations
- Target Type (e.g., sabotage, theft)
- Target Sets

Terminology Comparison: The Safety-Security Interface

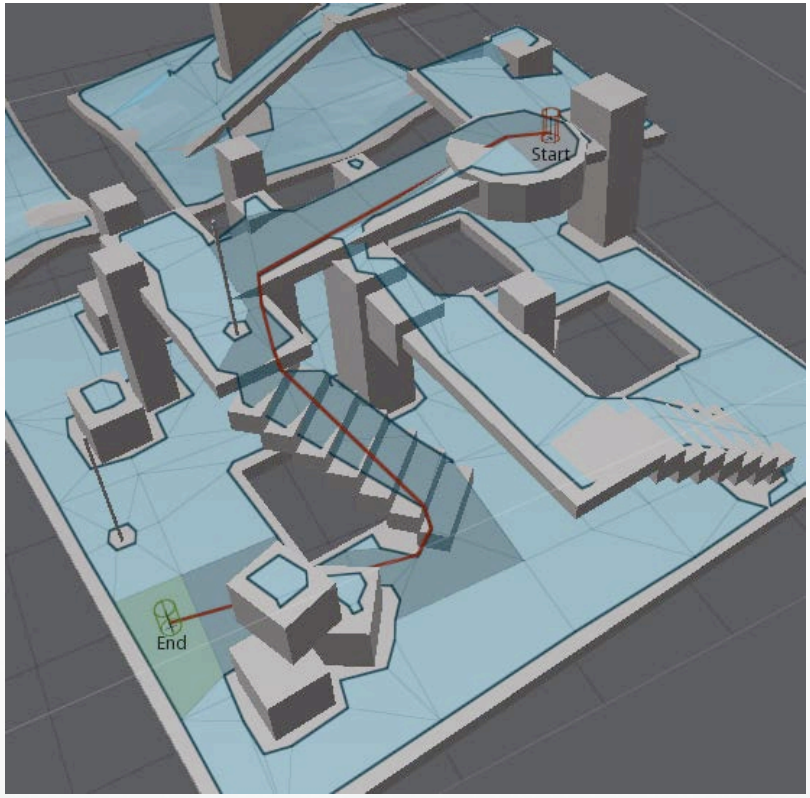
PSMS	PSA	Comments
Security Virtual Environment (SVE)	N/A	PSA has attempted some automation of P&IDs to system FTs, but with limited utility.
Adversary/Agent Traversal Graph	Fault Tree/Event Tree Logic	The adversary graph can be determined automatically from the SVE while the FT/ET logic is developed by a risk analyst.
Performance Data Library	Failure Rate Database	PSMS can directly adapt PSA analysis techniques for using historical data (generic and site-specific) to estimate performance.
Target Sets	Minimal Cutsets	Minimal cutsets along with spatial information are used to generate target sets.
Threat Scenarios	Initiating Events (IEs)	**The most significant difference between PSA and PSMS approaches are in the treatment of the random IEs vs. the intentional acts of an adversary.**
Risk $R_k = f_k \sum_{j=1}^{m_k} l_j * c_j$	Same as PSMS	Definition of risk is the same for a given threat scenario/initiator, but with PSMS conditional likelihood l_j, coming from simulation, and with f_k and c_j, commonly set to unity.

The Adaptive Adversary

<u>Goal:</u> Identify and prioritize the possible steps (i.e., paths) a given threat could use to defeat the security system and determine the corresponding likelihood of adversary success

General Steps:

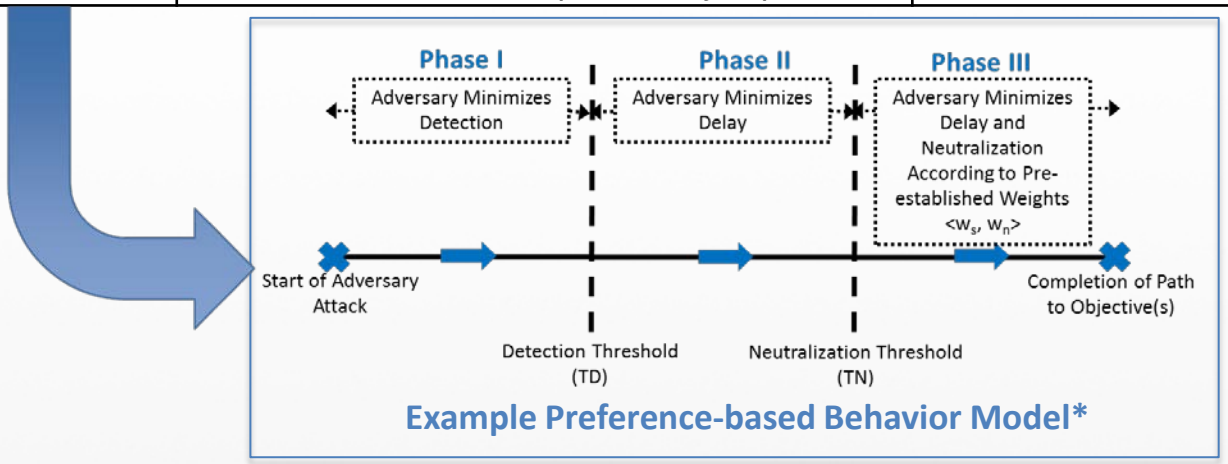
1. Break Security Virtual Environment into a data structure (e.g., navigational mesh, ASD) that a behavior model can use for adversary pathfinding
    - Possible pathways represented by mathematical graphs (nodes and edges) analogous to event trees (events and split fractions) in PSAs.
2. Solve graph to find the adversary pathways of greatest vulnerability to the facility
    - These vulnerabilities become the adversaries' "attack plans."
3. Virtually attack (i.e., simulate) the facility using this attack plan, but allow adversary to **adapt** to conditions on the ground that could not have been known during planning
4. Divide the number of successful attacks by the total attacks simulated to give the likelihood of adversary success



Example Navigational Mesh and Pathway

Behavior Model Determines Whether Adaptations Are Believable

Model	Description	Application
Task-based Models	Adversaries must accomplish pre-determined mission tasks, as defined by Subject Matter Experts (SMEs), but are free to determine how these tasks are accomplished and to locally adapt routes between these tasks.	Used throughout DOE's existing nuclear facilities where vulnerabilities are well understood and required adversary tasks are well defined. Only PSMS approach addressed in NUREG/CR 7145.
Preference-based Models	Adversaries are free to search globally for the "best" routes and tasks (i.e., paths) based upon their defined preferences (e.g., detection, delay, neutralization), but modeling requires more data and searches can be computationally expensive.	Can be used for searching for "new" vulnerabilities and "unanticipated" adaptations. Especially useful for less "hardened" facilities and during initial facility design.



Example Preference-based Behavior Model*

*Fogarty, S. P., "An Improved Model for Adversary Decision-making through Modeling and Simulation", Proceedings of the 57th Annual Meeting of the Institute of Nuclear Materials Management, forthcoming.

Sources of Modeling Uncertainty

PSMS analysis provides a means to address these key uncertainty contributors that are present in the security systems of today.

Source	Description
Decision-making on officer deployment	Details of how officers are deployed can be left to shift tactical commanders (STCs) and these commanders can make different decisions all within a given response plan.
Failure of security system components to function as designed	Random failure of any system components (including officers). The failure modes for equipment components are generally knowable. This is not failure due to the adversary defeating the components (that failure is integral to the simulation), but rather an unrepaired/latent failure prior to attack. Common use of compensatory measures exacerbates this issue.
Operating Modes and Target Sets	This is the uncertainty in the modeling of the defined operating modes (e.g., full power, refueling) of the facility. Some operating modes may occur only infrequently, but may represent increased vulnerability due to target set exposure or security design configuration.
Environmental Conditions	This is uncertainty in the modeling of environmental conditions. Only choosing to model daytime operations in the summer are examples of this insufficient modeling uncertainty.

Example: Failures in the Security System

July 2012 incident at DOE's Y-12 facility: Three protestors were able to breach the perimeter of the high security facility and deface the building prior to being interdicted by the protective force.

- Equipment side: A critical assessment camera had been inoperable for an extended period of time.
  - In addition a historically high nuisance alarm rate (caused by animals, winds, etc.) contributed to desensitizing the central alarm systems operators.

- Human performance side:
  - Slow response by the primary assessment patrol
  - Failure of the alarm station operator to declare a high priority (immediate) response based on the activation of three separate alarm sensors

Reinforces the benefit of PSMS for addressing this risk contributor

Risk Informing Security Decisions with PSMS

Given the similarities between PSA and PSMS analyses it is natural to look at the current risk informed decision process (RG 1.174) as a template for risk-informing security.

Define Proposed Change

PSMS could/should be used to assist in change definition as well.

Perform Analysis

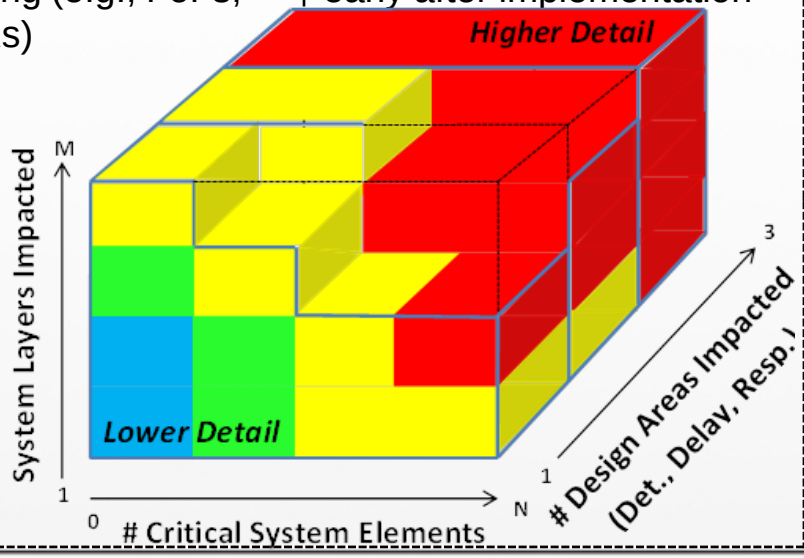
Includes PSMS and other limited and full-scope performance testing (e.g., FoFs, TTXs)

Define Implementation /Monitoring Program

Ensure that any unanticipated issues with the change are identified early after implementation

Document and Submit Change (as required)

Documentation for each analysis that was conducted to support the decision, as well as the decision document (e.g., 50.54p) that explains how all the analyses integrate together to support the change.



Nuclear Experience with PSMS

DoD

- Approach is generally centralized – hub-and-spoke model (e.g., DTRA as “hub”)
- Individual military bases and security force units typically don’t have in-house expertise or local access to PSMS software tools
- Services generally use PSMS intermittently compared to DOE
- Selected efforts at using PSMS internationally with NATO
- Have conducted PSMS tool Verification, Validation, and Accreditation

DOE/NNSA

- In-house “organic” risk assessment teams with expertise in PSMS fundamentals and the use of tools
- DOE/NNSA was an early adopter of PSMS and leads the community in the use of PSMS tools
- DOE sites typically employ more than a single PSMS tool
  - Allows sites to compare the results between software tools as well as performance tests
  - Effective but expensive approach (at least initially)
- Existing policies can make it difficult to adopt new approaches

Going Forward

- Limited guidance on implementation process and quality expectations for modern PSMS, resulting in uncertainty on how to address:
  - Modeling uncertainties (e.g., operating modes, system failure)
  - Sensitivity analysis (e.g., Critical System Elements, Defense-in-Depth)
  - Referenceable performance data
  - Peer review
- No common library of security performance data
- Limited quantitative analysis skills resident in the licensees' security organizations
  - PRA analysts might be trained for these efforts including providing the associated technical basis documentation
- Applications to date are tool-centric rather than deliverable/decision-centric
- Natural tendency to compare safety risks (i.e., PSA) to those from security (i.e., PSMS)
  - Some normalization of assumptions is needed
  - Cannot continue to set consequences and attack frequency to unity

HARVARD Kennedy School
BELFER CENTER
FOR SCIENCE AND INTERNATIONAL AFFAIRS

Complexities of Vulnerability Assessment

Matthew Bunn
Professor of Practice, Harvard Kennedy School
Advisory Committee on Reactor Safeguards, NRC
6 April 2016
belfercenter.org/managingtheatom

Computer tools for vulnerability assessment are extremely helpful

- Computer tools, if properly developed and used, allow:
  - Higher fidelity in simulation
  - Greater ease in considering different security options (can identify cheaper, more efficient solutions)
  - Greater ease for regulators seeking to confirm effectiveness of proposed exemption approaches
  - Greater ease in exploring new adversary pathway scenarios (can lead to more complete coverage of potential vulnerabilities)
  - Greater ease in considering impact of changes in adversary capabilities, tactics (can make it possible to assess impact of potential changes to the DBT, design systems to offer some protection against threats beyond the DBT)

But it is crucial to understand the limits of these tools

- "All models are wrong. Some are useful." Some can also be dangerous – they can create false impressions that all key factors are included
- Vulnerability assessment models are useful for identifying factors to be addressed, approaches to address them
  - NOT likely to provide reliable absolute estimates of risk, because of large uncertainties and complexities
- Key complexities and uncertainties include:
  - Complexity of overall security system
  - Limited by assessor's ability to think of complete set of defeat strategies adversaries could use effectively
  - Human and organizational factors usually poorly modeled
  - Insider threats more difficult to model
  - Cyber threats (and integrated cyber-physical threats) more difficult to model

Key assumptions built into vulnerability assessment tools

- Technological elements will perform as estimated
- Humans and organizations will perform as estimated
- Adversary capabilities and tactics will be within the DBT
- Adversaries will not use defeat strategies the defense has not thought of
- Any of these assumptions could turn out to be wrong
  - Technology my be improperly installed, operated, maintained
  - Humans may become complacent, organizations may put priorities elsewhere
  - Adversaries may be beyond the DBT
  - Adversaries may defeat the system with unimagined strategies

1: Difficult to model complex systems

- Security systems include many elements
  - Technical elements (e.g., barriers, cameras, alarms)
  - Human and organizational elements
  - Interactions among elements are complex and poorly understoodd – e.g., under what circumstances will employees report concerning behavior? What factors lead to complacent behaviors that undermine system performance?
- Y-12 example:
  - Installation of ARGUS system intended to improve security – but led to many unexpected false alarms
  - Cameras to check alarms had been broken for months
  - Guards had gotten sick of checking out false alarms
  - Result: protestors penetrated to HEU building, spent substantial period there, before being accosted by a single guard
  - Vulnerability assessment tools would not have shown problems

2: Difficult to imagine adversary tactics

- Tools are only as good as the people who use them
- Need creative, “hacker” mentality to envision approaches adversaries may use to defeat security systems
  - Real systems have many potential vulnerabilities – most of which will never be discovered, either by defenders or by adversaries
  - Partial solution: operators should establish “red teams” assigned to find vulnerabilities – and rewarded for doing so

3: Difficult to model human, organizational behavior over time

- Tools typically include simple assumptions on human performance based on past data
  - E.g., probability of detection for a guard in a guard tower
- Changes in security culture, organizational priorities change performance in hard-to-predict ways
  - How well will guards assess, respond to alarms?
  - How likely is it that staff will report behaviors that might reveal an insider threat?
  - What fraction of security rules will be followed, and implemented correctly?
  - What corners will be cut as production or budget pressures increase?
  - How will staff training, experience, security awareness change over time?

Security culture matters: Propped-open security door

Source: GAO, Nuclear Nonproliferation: Security of Russia's Nuclear Material Improving, Enhancements Needed (GAO, 2001)

4: Insider threats are difficult to model

- Computer tools typically do better modeling protection against outsiders
  - Traditional methods based on detection probability, task time, response force arrival time work better for outsider scenarios
- Insiders start off past many layers of defense – and may pursue hard-to-predict strategies
  - Insiders may be deeply familiar with the security system and its weaknesses – may have months or years to think, plan, experiment
  - Insiders have many opportunities for "social engineering" – convincing other staff to do seemingly harmless things that facilitate the plot
  - Insiders may recruit or coerce other insiders (few DBTs include multiple insiders, but in major non-nuclear thefts, multiple insiders are common)

5: Cyber threats are difficult to model

- Cyber threat environment evolving at frightening speed
- Cyber vulnerabilities are often unknown until exploited by an adversary
- Interactions between cyber threats and physical threats are complex and difficult to model
  - Systematic assessment of cyber-physical threat interactions is in its infancy, requires further development

Use computer tools – while being aware of their limitations

- DOE and DOD have used computer vulnerability assessment tools for many years to good effect
  - Have helped strengthen effectiveness and efficiency
- But need to avoid undue reliance
  - Results are no better than the assumptions that went into the model – some of which may be wrong
  - NRC should use expert judgment to decide whether to grant an exemption based on a computer analysis
  - As NRC shifts toward more performance-based approaches, realistic testing of security performance – including an effective force-on-force exercise program – will be critically important

Similarly, be careful in relying too much on material attractiveness

- Absolutely makes sense to adjust security requirements for material that would be very difficult to use for a nuclear bomb
- But current NRC staff proposal goes much too far
  - If material was less than 10% by weight Pu-239 or U-235, licensees could have a security plan based on adversaries stealing the material and local law enforcement recovering it
  - This degree of reliance on material dilution is contrary to decades of U.S. studies (including by NRC) that concluded recovery of pure material was straightforward enough that moderate dilution alone did not justify major security reductions
  - Would likely result in the United States having the weakest rules in the world for security for MOX fuel – wrong direction to lead
  - Public comment available:

    http://pbadupws.nrc.gov/docs/ML1429/ML14293A636.pdf