SAND2018-6151C

Summary of a Sandia National Laboratories Workshop on Extended Probabilistic Risk Assessment (ePRA)

Robert Forrest[1], Jason Reinhardt[1], Timothy Wheeler[1], Adam D. Williams[1]

[1]Sandia National Laboratories, Albuquerque, NM, USA, [rforres, jcreinh, tawheel, adwilli]@sandia.gov*

Fifty years ago, it was realized that the complexity of operating large-scale nuclear power plants (NPP) necessitated new mechanisms for identifying, measuring and assessing the risk of undesired events—resulting in the development of probabilistic risk assessment (PRA) as a generally agreed to framework for addressing the safety risks of nuclear power. Safety-focused risk analysis and assessment approaches, however, struggle to adequately address malicious acts against nuclear material, infrastructure, and facilities and non-proliferation issues. Yet, responding by treating safety, security, and safeguards concerns independently is inefficient. At best, this assumption may not take explicit advantage of measures that provide benefits against multiple risk domains, and, at worst, it may lead to implementations that increase overall risk due to incompatibilities.

What is needed is an integrated safety, security and safeguards risk (or "3SR") framework for describing and assessing nuclear power risks that can enable direct trade-offs and interactions in order to inform risk management processes — a potential paradigm shift in risk analysis and management. In an ideal future, regulators, nuclear power plant operators, and designers will utilize a unified analysis framework to inform decision making processes and to understand overall risks across the domains of safety, security, and safeguards—perhaps in terms of an "extended probabilistic risk analysis" framework, or ePRA.

This conference paper summarizes the proceedings of a Sandia National Laboratories-hosted Workshop on Extended Probabilistic Risk Assessment (ePRA) in August 2017 as an attempt to begin the discussions to move towards a 3S Risk approach. Further, this paper reviews the historical approaches, current challenges and modern approaches to nuclear power risk assessment presented at the workshop. It will then discuss key challenges and takeaways identified by the participants. Ultimately, this paper provides a notional research agenda to improve risk assessment for the nuclear energy discipline.

INTRODUCTION

Fifty years ago, it was realized that the complexity of operating large-scale nuclear power plants (NPP) necessitated new mechanisms for identifying, measuring and assessing the risk of undesired events. U.S. Senator John Pastore's 1971 letter to Atomic Energy Commission chairman James Schlesinger proposed that an assessment be performed to understand the probabilities and consequences across a range of possible accidents. Senator Pastore made this suggestion in order to begin addressing mounting concerns around nuclear power plant safety. Over the next three decades, a large community of nuclear power engineers, scientists, academics, and regulators coalesced around a set of commonly held assumptions, definitions, and standard quantitative analytical tools that allowed for safety risks to be assessed and used to inform safety-related regulatory and policy deliberations. The general agreement of a framework for considering these safety risks allowed for an improved ability to manage nuclear power safety.[1]

* **SAND2018-XXXX.** Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Yet, safety-focused risk analysis and assessment approaches struggle to adequately include malicious, deliberate acts (e.g., terrorist acts or protestors) against the nuclear power industry's fissile and waste material, infrastructure, and facilities. Further, existing methods do not adequately address non-proliferation issues (e.g., nuclear material diversion). Treating safety, security, and safeguards concerns independently is inefficient because, at best, it may not take explicit advantage of measures that provide benefits against multiple risk domains, and, at worst, it may lead to implementations that increase overall risk due to incompatibilities. In an ideal future, regulators, nuclear power plant operators, and designers will utilize a unified analysis framework to inform decision making processes and to understand overall risks across the domains of safety, security, and safeguards—and "extended probabilistic risk analysis" framework, or ePRA. However, developing such a framework is challenging prospect and there is currently little agreement on how security related risk factors, such as adversary decision making, should be handled in risk analytic methods. What is needed is an integrated safety, security and safeguards risk (or "3SR") framework for describing and assessing nuclear power risks that can enable direct trade-offs and interactions in order to inform risk management processes — a potential paradigm shift in risk analysis and management.

This conference paper summarizes the proceedings [1] of the Sandia National Laboratories-hosted Workshop on Extended Probabilistic Risk Assessment (ePRA), held August 22-23, 2017, as an attempt to extend the discussions and deliberations on how to augment safety focused risk assessment approaches to include security concerns and begin moving towards a 3S Risk approach. (NOTE: Given the increased complexity of including them, safeguards concerns were not included in this initial workshop and are left to future efforts.)

HISTORICAL APPROACHES & CURRENT CHALLENGES

After Senator John Pastore's 1971 letter to Atomic Energy Commission set the nuclear power community on the path of using probabilistic risk analyses (PRA), the focus evolved to consider higher frequency, smaller consequence events instead of just rare, massive failures. Further maturation occurred in the next decades, such as the adoption of Bayesian methods and plant-specific PRAs. More modern methods use a risk-informed approach, a combination of a deterministic approach and a risk-based approach. This more modern way of thinking resulted in current "Deliberative Decision Making Processes" where technical analysis is considered as one of a broad spectrum of decision making criterion. A broad spectrum of current risk assessment approaches is available to analysists—which can be summarized in a handful of categories, as shown in Table 1.[3]

With such a broad array of approaches available, it is important to fundamentally understand the questions being addressed, and the implicit and explicit assumptions that are made when choosing an approach. No one approach is "correct" in any absolute sense—each approach has benefits and drawbacks. By moving to a 3SR framework for risk management, a mature nuclear power enterprise is likely to use a such a set of approaches, inclusive of newer methods discussed below, resulting in a risk management approach wherein the security analysis contributes one part of a deliberative dialogue to decision making.

Table 1. Summary of Current Risk Assessment Approaches (summarized from [3])

Risk Analysis Categories	Description
Prescriptive Requirements & Best Practice Lists	A set of measures that provide clear guidance for implementation and compliance
Ad-Hoc Risk Assessment & Management	Structured approaches to subject matter expertise that provide a more adaptive approach and facilitate an ongoing dialogue on risks
Disciplined Qualitative Risk Assessment	Structured methods for developing scenario sets and careful consideration of relative likelihoods, and consequences
Vulnerability Analysis & Penetration Testing	Methods that generate important but otherwise difficult to imagine scenarios (that can validate other analyses)
Design Basis Threats	Related to the Design Basis Accident that provides guidance/ acceptance criteria against which to design/operate related systems
Frequentist Probabilistic Risk Assessment	Methods that use historical hazard data to assess probabilities of particular scenarios—especially when data sources are well known
Bayesian Probabilistic Risk Assessment	Set of mathematically rigorous methods to manage uncertainty and make risk-informed decisions

There are several challenges that must be addressed when moving beyond safety focused PRA approaches to integrate security concerns and move towards a 3SR framework. Unlike the evolution of the safety PRA methods, security assessments have yet to go through the debate and consensus building that is required to create and accept a standard set of approaches. The community does not yet have a shared understanding or history of thought. Additionally, while safety is the responsibility of the nuclear power community, security is a shared responsibility with the government in terms of national, regional and local investments in law enforcement. What's more, passive safety systems offer measures of protection not captured in traditional approaches to security analysis. Moving forward, security assessments need a way to rationally credit these built in aspects of security and not assume the security of reactors exists in isolation.

Several other challenging elements of risk assessment must be addressed in order to move towards a 3SR framework by integrating safety and security risk assessments. First, adversary modeling presents a significant challenge to security risk assessments that utilize the Threat, Vulnerability and Consequence construction of understanding risk—including the large uncertainty on the probability of adversary actions and the ability for intelligent adversaries to adapt their plans. Not only do security assessments become interdependent on adversary choice and options, but consequences feed back into adversary decision making and therefore create a complex non-linear decision making system. Second, the move away from analogue technologies toward more digital assets and the consideration of new reactor technologies increases the complexity of risk assessments. The increasing number of interdependencies may challenge classic PRA logic. For example, methods and applications of risk assessments in the cybersecurity realm are not well-understood and the focus of a significant body of current research. Unless new methods that can address these complexities are developed, the magnitude of the effort required to fully analyze the integrated set of risks and systems may with current approaches become prohibitively expensive and fail to deliver timely results.

Third, well defined, measurable, and actionable metrics are needed for robust risk management, but it's often not clear what metrics are appropriate for integrated assessments—for example, there is no

security corollary for "quantitative health objectives" in nuclear safety. A central metric would make implicit trade-offs between each of the 3SR concepts that must be carefully considered. Additionally, it is important to understand both adversaries and defenders may be simultaneously successful if their definition of success do not align. Finally, it will be important to consider approaches to capturing (either qualitatively or quantitatively) the sociological impacts of safety and security decisions in nuclear power risk management in a 3SR framework.[4] Lastly, there is the historical challenge in the nuclear power community of considering cultural issues. Decision makers have an expanded scope of considerations beyond just technical risk assessment results. This insight led to the so-called "risk-informed approach" of decision making wherein technical analysis is one of a larger suite of considerations for a decision maker. Both technical and social value judgements must be considered in the risk assessment and management process. Finally, the distance between the actual risk of harm and the broader perception of risk of harm is a problem that may become exacerbated when safety and security assessments are integrated.

MODERN APPROACHES

Despite the formidable challenges discussed in the previous section, there are productive efforts to address them currently underway that were discussed in the workshop. These approaches, summarized in Table 2, may offer fruitful and incremental steps towards the integration of safety and security risk assessments and a 3SR risk management framework.

Modern Approaches	Description
Success Paths	An approach that considers the actions, systems, and components necessary for barrier success—as opposed to the probability of adversary success [5]
Predictive Risk	Methodologies intended to model an adversary's preferred choice of action based on a "strategy tree" and a consumer selection model [6]
Difficulty Based Assessments	A focus on how difficult it would be for an adversary to accomplish the necessary tasks for a successful attack and a "path of least resistance" assumption [7]
Optimization Methods	Approaches aimed to align the efficiency and effectiveness of designing and deploying risk mitigating measures for safety and security [8]
Cybersecurity Assessments	Currently borrow the philosophy and application of defense in depth strategies to protect critical cyber systems [9]
Integrating Safety and Security Risk Assessments	Recent efforts that have attempted to integrate safety and security risk assessments using dynamic probabilistic risk assessment and system theoretic process analysis and concluded that such techniques better incorporate multi-faceted interactions in risk analysis [10]

As a 3SR risk assessment and management approach is developed in the nuclear power community, similar approaches should be used in order to leverage similarities across the safety, security, and safeguards domains whenever possible.[11] A review of conflicts and synergies between safety and security analyses highlights other insights that can guide the development of 3SR frameworks. For example, while a safety analysis would consider accident scenarios, the system response, and associated consequences, a security analysis would have a parallel structure of threats, system response, consequences. There are additional intrinsic features that increase synergies between physical security and safety. For example, certain passive safety systems that do not need routine

surveillance or maintenance, can be placed in hardened locations that are difficult to access. Barriers that provide defense–in-depth to radiological release also provide physical security barriers, with the AP1000 passive design as a possible example. Quantitative assessments of safety and security risks that combine a currently rare, but have been attempted with promising initial results.[12] Exploratory, early-phase research and development on methods to both unravel and understand the complex interdependencies and provide integrated assessments of safety and security risks will be necessary to advance towards a 3SR risk management framework.

KEY CHALLENGES, TAKEAWAYS & POTENTIAL NEXT STEPS

During the ePRA workshop, the participants identified a set of key challenge, which included:

- *3SR Metric Integration*—creation of metrics must be used to translate between safety and security which intrinsically necessitates a value judgement between safety and security. However, a debate remains as to the validity of making such value judgements in the first place, and if doing so undermines the technical validity of the analysis.

- *Relative and Absolute Risk*—integrating subjective metrics often produces results containing a relative risk. While the integration of such methods with quantitative results runs up against the 3SR metric integration problem, there is a debate as to the fundamental validity of relative risk.

- *Security Assessment Tools*—using safety risk assessment tools for security has historically faced challenges. Because of intrinsic differences, for example in adversary modeling, it has yet to be determined if security assessment will ever reach the state of maturity of safety PRAs.

- *Integration or Framework*—there remains a debate on if it is possible to formally integrate safety and security risk assessment techniques, or will the field move to a framework of integrating several, disparate analysis into a larger risk assessment and decision making framework.

- *Risk Perception*—one key in analyzing risk is the difference in public perception and objectively measured risk assessments. Decision makers are hesitant to recommend consequence reduction solutions for security scenarios. It is an open question as to if these should be incorporated into analysis or left to decision makers to accept additional risk based on cultural values.

In response, the workshop participants also identified a set of key takeaways and questions that need to be address, which included:

- *Security PRAs lack of maturity*—lagging 20 years behind safety PRAs, the nuclear risk community does not have a mature an understanding of security risk. There, how can we develop the field in conjunction with safety as opposed to thinking of them as separate and combining them later?

- *Utility Comes in Understanding What You Don't Need*—the sign of maturity for this field may be in understanding and justifying measures that don't contribute significantly to safety and security. Therefore, what result does this change from my traditional PRA? What requirement do I no longer need?

- *Begin by Emphasizing Similarities between Safety and Security*—reconciling and leveraging similarities first, then move into integrating differences. Therefore, what security benefits of passive cooling and containment of new nuclear reactors exist? [11] How can these lessons be extended?

- *Cyber Touches Everything*—because it touches safety, security and safeguards, cyber risk can be thought of as the first regime in which safety and security must be integrated by necessity. Therefore, how can better understanding cyber risk be an entry point to understand how to integrate more traditional analysis? [6]

- *Cyber Complexity Mimics Safety and Security Complexity*—cyber issues quickly become unwieldly and combinatorics makes traditional fault tree analysis unsustainable—which mimics the complexity of integrating safety and security analysis. Therefore, how could new concepts, tools, and techniques required for cyber also enhance integrating safety and security?

- *Success Paths*—thought of roughly as the opposite of fault trees, are a useful tool to quickly understand potential safety/security containment requirements. Therefore, how can similar concepts and tools address the previously described issues of increased complexity of modern analysis?

- *Culture and Sociological Issues*—as safety and security integration progresses, new cultural and sociological issues may arise that trump technical concerns. Therefore, how can the technical risk community constantly acknowledge and work to address these issues?

At the end of the workshop, the participants discussed a notional research agenda and potential next steps to maintain the positive momentum in this conversation on an integrated approach to the security, safety, and safeguards risks of nuclear energy. In the ***short term*** (0-3 months), this included:

- *Coordinate a core technical team* to contribute time and effort in the near future to push and advocate for continuing down the path outlined by the workshop. Build up a community, have a set of sessions dedicated to continuing the conversation.

- *Complete a Literature Review* to survey ALL risk-related analysis techniques, approaches and tools throughout the complex (and sample those from beyond). It would need to be a wide survey of conceptual approaches to risk, given that most of this literature is adversarial modeling, but we would have to widen range to include integration methods.

- *Identify Customer Need(s)* to characterize metrics that would be useful. Have potential customers review the ideas and any initial products.

- *Develop a Technical Roadmap* to organize and develop the insights guide the group and serve as a project plan.

In the ***medium term*** (3-6 months), this included:

- *Holding an Additional "Working" Workshop* to select 2-3 approaches to test for integrated risk assessment from the literature. As this goes forward, we should consider including members of the ASME & ANS Joint Committee on Nuclear Risk Management (JCNRM).

- *Work Through One Example* to identify a manageable set of scenarios on which to evaluate risk from an "integrated" perspective. Technical team may address key needs and issues listed in this workshop.

In the ***long term*** (0-3 months), this included:

- *Evaluating Scenario Work* to expand the evaluation of the scenario(s) from above, including the potential to conduct another inter-lab workshop to discuss results, conduct an internal (and/or external) peer review, and then plot further action based on these results.

REFERENCES

[1] Apostolakis, George, "Historical Perspectives and Current Issues," Presented at 2017 Sandia National Laboratories' Extended Probabilistic Risk Assessment Workshop, August 2017.

[2] Forrest, R., Reinhardt, J., Wheeler, T., and Williams, A. (2017) *A 3S Risk Assessment Approach for Nuclear Power: Safety, Security, and Safeguards (SAND2017-11989)*, Sandia National Laboratories, Albuquerque, NM.

[3] Wyss, Gregory, "Survey of Security Risk Assessment Examples," Sandia National Laboratories, Presented at 2017 Sandia National Laboratories' Extended Probabilistic Risk Assessment Workshop, August 2017.

[4] Clark-Ginsberg, Aaron, "Assessing Electric Grid Cybersecurity Risks: Three Ideas from Disaster Sociology," Stanford University, Presented at 2017 Sandia National Laboratories' Extended Probabilistic Risk Assessment Workshop, August 2017.

[5] Grabaskas, Dave, "Advanced Reactor PRA Analytics," Argonne National Laboratories, Presented at 2017 Sandia National Laboratories' Extended Probabilistic Risk Assessment Workshop, August 2017.

[6] Unwin, Steve, "A Threat Methodology: Application to Emerging Technologies," Idaho National Laboratories, Presented at 2017 Sandia National Laboratories' Extended Probabilistic Risk Assessment Workshop, August 2017

[7] Wyss, Gregory, "Risk Assessment vs. Risk Management," Sandia National Laboratories, Presented at 2017 Sandia National Laboratories' Extended Probabilistic Risk Assessment Workshop, August 2017.

[8] Brown, Nate, "A Stochastic Programming Approach to the Design Optimization of Layered Physical Protection Systems," Sandia National Laboratories, Presented at 2017 Sandia National Laboratories' Extended Probabilistic Risk Assessment Workshop, August 2017.

[9] Muhlheim, Michael, "I&C System Design and Cyber-Security Safeguards," Presented at 2017 Sandia National Laboratories' Extended Probabilistic Risk Assessment Workshop, August 2017.

[10] Williams, A.D., D. Osborn, K. A. Jones, E. A. Kalinina, B. Cohn, A. H. Mohagheghi, M. DeMenno, M. Thomas, M. J. Parks, E. Parks and B. Jeantete. (2017) *System Theoretic Frameworks for Mitigating Risk Complexity in the Nuclear Fuel Cycle: FINAL REPORT (SAND2017-10243)*, Sandia National Laboratories, Albuquerque, NM.

[11] Peterson, Per, "PRA Synergies in Safety, Security, and Safeguards," University of California Berkeley, Presented at 2017 Sandia National Laboratories' Extended Probabilistic Risk Assessment Workshop, August 2017.

[12] Williams, Adam D., "Exploring Risks Associated with the Global Expansion of Civilian Nuclear Power," Sandia National Laboratories, Presented at 2017 Sandia National Laboratories' Extended Probabilistic Risk Assessment Workshop, August 2017.