SANDIA REPORT
SAND2017-11898
Unlimited Release
Printed September 26, 2017

A 3S Risk Assessment Approach for Nuclear Power: Safety, Security, and Safeguards

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

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

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.

[1] **Contact:** rforres@sandia.gov; +1 (925) 294-2728


Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology and Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

SAND2017-11898
Printed September 2017
Unlimited Release

A 3S Risk Assessment Approach for Nuclear Power: Safety, Security, and Safeguards

Robert Forrest[2]
Jason Reinhardt
Timothy Wheeler
Adam Williams
Sandia National Laboratories
P. O. Box 5800
Albuquerque, New Mexico 87185

Abstract

Safety-focused risk analysis and assessment approaches struggle to adequately include malicious, deliberate acts against the nuclear power industry's fissile and waste material, infrastructure, and facilities. Further, existing methods do not adequately address non-proliferation issues. 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. 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.
These proceedings of the Sandia ePRA Workshop (held August 22-23, 2017) are an attempt to begin the discussions and deliberations to extend and augment safety focused risk assessment approaches to include security concerns and begin moving towards a 3S Risk approach. Safeguards concerns were not included in this initial workshop and are left to future efforts. This workshop focused on four themes in order to begin building out a the safety and security portions of the 3S Risk toolkit:

1. **Historical Approaches and Tools**
2. **Current Challenges**
3. **Modern Approaches**
4. **Paths Forward and Next Steps**

This report is organized along the four areas described above, and concludes with a summary of key points.

[2] **Contact:** rforres@sandia.gov; +1 (925) 294-2728

TABLE OF CONTENTS

1. Introduction 8
2. Historical Approaches and Tools 9
    - 2.1.1. Prescriptive Requirements and Best Practice Lists 9
    - 2.1.2. Ad-Hoc Risk Assessment and Management 10
    - 2.1.3. Disciplined Qualitative Risk Assessment 10
    - 2.1.4. Vulnerability Analysis and Penetration Testing 10
    - 2.1.5. Design Basis Threats 10
    - 2.1.6. Frequentist Probabilistic Risk Assessment 10
    - 2.1.7. Bayesian Probabilistic Risk Assessment 11
3. Current Challenges 11
    - 3.1.1. Adversary Modeling 11
    - 3.1.2. Technical Complexity 12
    - 3.1.3. Metrics Identification 12
    - 3.1.4. Cultural Considerations 12
4. Modern Approaches 13
    - 4.1. Success Paths 13
    - 4.2. Predictive Risk 13
    - 4.3. Difficulty Based Assessments 13
    - 4.4. Optimization Methods 14
    - 4.5. Cybersecurity Assessments 14
    - 4.6. Integrating Safety and Security Risk Assessments 14
5. Key Challenges and Takeaways 15
    - 5.1. Key Challenges 15
    - 5.2. Key Takeaways 16
6. Paths Forward and Next Steps 17
    - 6.1. Short Term (0-3 months) 17
    - 6.2. Medium Term (3-6 months) 18
    - 6.3. Long Term 18

Appendix A: References 19

Appendix B: Workshop Attendees 21

1. INTRODUCTION AND SUMMARY

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 next three decades, a large community of nuclear power engineers and scientists, academics, and regulators coalesced around a set of commonly held assumptions, definitions, and standards 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.[3]

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. 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. One might think of this as an "extended probabilistic risk analysis" framework, or ePRA. However, developing such a framework is a challenging prospect. It took many years for the nuclear power community to fully adopt and craft a suite of quantitative risk approaches that could be integrated into regulatory decisions and safety investments. There is currently little agreement on how security related risk factors, such as adversary decision making, should be handled in risk analytic methods. Further, the debate is ongoing as to how to integrate risk metrics and what risk levels are acceptable. Through the discussion and debate the nuclear power community developed a common frame in which to view both the analysis and the results. Those methods are still being revised as new reactor technologies are being considered and new information about failure modes and plant performance is being discovered.

These proceedings of the Sandia ePRA Workshop (held August 22-23, 2017) are an attempt to begin the discussions and deliberations to extend and augment safety focused risk assessment approaches to include security concerns and begin moving towards a 3S Risk approach. Safeguards concerns were not included in this initial workshop and are left to future efforts. This

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

workshop focused on four themes in order to begin building out a the safety and security portions of the 3S Risk toolkit:

1. **Historical Approaches and Tools:** Participants reviewed a sampling of current approaches to both safety focused PRAs and attempts to address security dimensions as well.
2. **Current Challenges:** Participants discussed the challenges of incorporating security threats into quantitative risk assessment methodologies.
3. **Modern Approaches:** Workshop participants identified and discussed current efforts to address the challenges posed.
4. **Paths Forward and Next Steps:** Finally, participants discussed possible steps forward, and research agendas that could contribute to the development of risk analysis methods that consider both safety and security in common frame.

This report is organized along the four areas described above, and concludes with a summary of key points.

Challenges
Below, we elaborate in depth on challenges to be addressed to move the field forward. Generally, in terms of security safeguards, the community does not yet have a shared understanding and history of thought. Uncertainty in adversary modeling presents a significant challenge to security risk assessments, and the increasing number of interdependencies may challenge classic PRA logic. Also, identification and translation of metrics between security and safeguards represents a fundamental problem in integrating safety and security.

Next Steps
We suggest short, medium and long term next steps to address the challenges above. Starting with assembling a core technical team to review the literature and develop a roadmap in the short term, we propose holding a 'working' workshop in the medium term (3-6 months) where we can work through one example of an integrated analysis. In the long term, we can peer review the pilot integrated analysis and plot a longer tem roadmap based on the results.

While this report summarizes the presentations and discussions from all attendees the workshop (see Appendix A for a list of presentations made, and Appendix B for a list of attendees), it should be noted that any errors in this document belong to the author team, and not to the workshop participants.

2. HISTORICAL APPROACHES AND TOOLS

After Senator John Pastore's 1971 letter to Atomic Energy Commission set the nuclear power community on the path of using probabilistic risk analyses, 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, but often led only to more regulation and not the reduction of unnecessary conservatism in regulatory requirements. More modern methods use a risk informed approach, a combination of a deterministic approach and a risk based approach. Risk informed initiatives defined integrated

decision making processes using more of a cost/benefit approach. This more modern way of thinking leads to current 'Deliberative Decision Making Processes' where technical analysis is considered one of a broad spectrum of decision making criterion. A broad spectrum of current risk assessment approaches is available to analysists.[4] Generally these can be summarized, along with the virtues and pitfalls of each, in handful of categories.

2.1.1. Prescriptive Requirements and Best Practice Lists

A set of requirements or best practices for safety or security measures can provide clear guidance for implementers and make it easier to assess compliance. However, these approaches are generally tied to specific types of systems, and are less adaptive, and respond more reactively to new systems or evolutions in threats and vulnerabilities.

2.1.2. Ad-Hoc Risk Assessment and Management

Risk assessments frequently begin with a brainstorming exercise focused on the question "what can happen, and how bad can it be?" Structured approaches to subject matter expert (SME) reviews can provide a more adaptive approach than static requirements and best practice lists, and facilitate an ongoing dialogue on risks. However, these approaches tend not to be validated and over-interpreted. They often rely on artificial rating scales that can provide an illusion of mathematical rigor.

2.1.3. Disciplined Qualitative Risk Assessment

Qualitative methods that offer structured methods for developing scenario sets and careful consideration of relative likelihoods, and consequences. However, these methods may not account for all the complexity required to precisely represent the logic of the problem, such as dependent events. Additionally, it is often difficult to easily compare results with other risks not explicitly covered in the analysis.

2.1.4. Vulnerability Analysis and Penetration Testing

These approaches typically use red-teaming techniques and hence rely on a rich adversary model in subject matter experts. Vulnerability analyses and penetration testing results often generate important but otherwise difficult to imagine scenarios, or can serve to validate other analyses to some degree. However, the results are often very narrowly focused on a specific component or installation, and it is difficult to be systematic enough to make broad statements about risks or regulatory requirements. Finally, the results rely on the quality of the experts used to perform the assessment, and may be subject ot mirroring biases.

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

2.1.5. Design Basis Threats

A Design Basis Threat (DBT) is related to the concept of Design Basis Accident (DBA) in that it provides guidance and acceptance criteria against which to design, install, and operate security systems. However, DBT approaches tend to assume a worst reasonable case for adversaries and do not consider the full spectrum of uncertainties. Prioritizations generally follow conditional risk assessments based on the assumption that a specific set of attacks will occur.

2.1.6. Frequentist Probabilistic Risk Assessment

Frequentist approaches to probabilistic risk assessment use historical hazard data to assess probabilities of particular scenarios. This can often provide a strong basis for assessing risk. There is well-established practice of decision making based on the PRA results when data sources are well known, and testing is used to provide valuable information. However, in security problems, it is common for little to no data to exist, and what data does exist may not be useful. Validation then becomes challenging, and subject matter experts must often make strong assertions to make results meaningful.

2.1.7. Bayesian Probabilistic Risk Assessment

As one of the most mathematically rigorous class of methods, Bayesian approaches provide powerful tools for managing uncertainty, and are well-established in safety and systems analysis. However, like other methods, extensions to security problems are less developed, particularly in the area of adversary modeling. Specifically, accounting for adversary adaptability is a significant challenge. This can make risk management decisions challenging, complex, and expensive.

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, and each approach has benefits and drawbacks. The suite of security risk assessment examples above should be looked at as an existing toolbox that can be applied to a problem. Ultimately, by moving to a 3SR framework for risk management, a mature nuclear power enterprise is likely to use a set of the above approaches, as well as newer methods discussed below, resulting in a risk informed approach to security wherein the security analysis contributes one part of a deliberative dialogue to decision making.

3. CURRENT CHALLENGES

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 and 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, security of passive safety systems is often already protected. Current security assessments need a way to rationally credit these built in aspects of security, and not assume reactors exist in isolation. In this section, we explore several other challenging elements of risk assessment that must be addressed in order to move towards a 3SR framework by integrating safety and security risk assessments.

3.1.1. Adversary Modeling

Adversary modeling presents a significant challenge to security risk assessments that utilize the Threat, Vulnerability and Consequence construction of understanding risk. When placing a probability on an adversary action in a security threat, some have concerns that the uncertainty on that probability is so large that it may not be not useful. Additionally, as security systems are developed, the adversary may shift towards other modes of attack. 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. The adaptability of adversary interactions complicates the risk assessment process.

3.1.2. Technical Complexity

In addition to the introduction of adversaries, 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. Methods and applications of risk assessments in the cybersecurity realm are not well-understood and the focus of a significant body of current research. Expanding risk management approaches for nuclear power to incorporate both digital assets and security concerns will be challenging, at best. 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 become prohibitively expensive and fail to deliver timely results. The default alternative analytical position may be more akin to Perrot's concept of Normal Accident Theory, and may prevent continued advancement in nuclear power technologies and utilization.

3.1.3. Metrics Identification

Metrics pose a fundamental problem in integrating safety and security. Well defined, measurable, and actionable metrics are needed for integrated assessments, but it's often not clear what metrics are appropriate. In safety, analysts consider 'quantitative health objectives', but there is no real corollary in security. Further, metrics that integrate safety and security concerns may have to overcome a problem of equity. A central metric would make implicit trade-offs between each of the 3SR concepts that must be carefully considered. After analyzing a scenario from safety, security and safeguard perspectives with different analysis techniques, analysts and decision makers must understand how to interpret metrics in some coherent way. Additionally, it is important to understand both adversaries and defenders may be simultaneously successful if their definition of success do not align. For example, if an adversary wants to deface a nuclear power plant, and the operator wants to prevent adversary access to nuclear materials, both parties may achieve their goals in an incident. 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.[5]

3.1.4. Cultural Considerations

A key point underlying most risk analysis are many aspects of cultural issues. This has been a historical issue in the nuclear power community. For instance, nuclear and mechanical engineers were not trained in probability and statistics. Abandoning a deterministic approach and using subjective metrics was often difficult to accept. In the context of integrating safety and security towards a 3SR risk management approach, cultural challenges are likely to persist. While consequence mitigation is often a reasonable method of reducing safety risk, the security community often views consequence mitigation as a nonstarter. Further, 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.

4. 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 may offer fruitful and incremental steps towards the integration of safety and security risk assessments and a 3SR risk management framework.

4.1. Success Paths

Success paths are part of a physical barriers approach that considers the actions, systems, components, that are necessary for the barrier to be successful, as opposed to considering the probability of adversary success.[6] The benefit of this approach is that it allows rapid system analysis and can lead to clearer communication of risk to decision makers. The approach is similar to fault tree analysis, but oriented differently; one determines what systems need to work to enforce barrier integrity. The examples demonstrate the ability to understand systems at any desired level of detail required. This approach allows the quick identification of vital systems or components, which can then be analyzed by more traditional risk analysis. Success path analyses are currently being applied in the analysis of immature reactor and plant designs by applying traditional concepts to increasingly prevalent passive safety systems.

[5] 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

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

4.2. Predictive Risk

Predictive risk methodologies are intended to model an adversary's preferred choice of action based on a 'strategy tree' and a consumer selection model.[7] This approach attempts to apply predictive risk to emergent technologies where no current experience base exists, and analysis must be based on an informed evaluation. The methodology identifies the barriers an adversary must overcome to achieve a goal, then determines the resources needed to overcome the barriers. Various models have been examined to understand which scenario is likely to be chosen by the adversary. Although it seems modeling the adversary as a consumer shows promise, it should be noted this is a method of understanding relative, not absolute risk.

4.3. Difficulty Based Assessments

Difficulty based assessments focus on how difficult it would be for an adversary to accomplish the necessary tasks to carry out a successful attack, and makes the assumption that an adversary would be more likely to choose a less difficult path.[8] This approach has been functionalized into a risk management method and set of tools and is currently used as a tool in several high-consequence sectors. The method combines scenario difficulty and consequences to evaluate a proxy for scenario risk. The resulting approach treats risk as the collection of all scenarios, their likelihood and consequences, and seeks to manage the collection as a whole. Similar to the predictive risk approach discussed previously, these risks informed are meant to focus on relative risk management, not measure of absolute risk.

4.4. Optimization Methods

While the analytical tasks are important, another critical component of risk management is optimizing the design and deployment of risk mitigating measures for safety and security. Current research is examining how to structure the design of security systems as optimization problems and determine optimum designs. Examples of this vein of research have been focused on the likelihood of adversary success given an attack by considering all possible paths an attacker could use to physically gain entry to an example facility.[9] Optimization routines are then be used to compare different mitigation strategies as well as intruder paths. This provides a very sophisticated adversary model, as well as method for assessing the overall effectiveness of security systems.

4.5. Cybersecurity Assessments

Integrated control systems (ICS) are relying more and more on connected digital assets presenting both safety and security concerns for the nuclear power community. A review of the

---

[7] 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
[8] Wyss, Gregory, "Risk Assessment vs. Risk Management," Sandia National Laboratories, Presented at 2017 Sandia National Laboratories' Extended Probabilistic Risk Assessment Workshop, August 2017
[9] 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

philosophy and application of defense in depth strategies to protect critical cyber systems, as well as historical incidents when outer layers of cyber architectures were breached can provide important insights. The evidence points to a performance based approach, as opposed to a prescriptive based approach, of providing assurance against cyber vulnerabilities.[10] Alternative views, such as focusing on the flow of information in cyber systems and assessing the risks associated with protecting that flow or taking success path approaches to cyber system analysis may also have merit.[11]

4.6. Integrating Safety and Security Risk Assessments

There have been some efforts that have attempted to integrating safety and security risk assessments, and have examined the problems in doing so. This includes a comparison of frameworks of integrating safety, security and safeguards for the specific scenario of spent fuel transport.[12] One framework, called Dynamic probabilistic risk assessment (DPRA), uses dynamic event trees that evaluated 3S risk by dynamically evaluating the interactions between uncertainties in real simulation time. A second framework called the System theoretic process analysis (STPA) is "A 'top-down' process that links specific design details to high-level objectives via hierarchy, emergence, interdependence & feedback" that evaluated 3S risk in terms of ensuring control over system behavior to avoid states of increased risk. One of the overall conclusions from the related LDRD study[13] was that these two system-theoretic techniques better incorporates multi-faceted interactions in risk analysis. Another potentially useful conclusion from that study related to a new paradigm wherein risk itself is considered complex, is described as a "state-space," and 3S risk management is a complex tradeoff between in implementation between meeting different performance requirements.

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 in across the safety, security, and safeguards domains whenever possible.[14] 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 the 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

[10] Muhlheim, Michael, "I&C System Design and Cyber-Security Safeguards," Presented at 2017 Sandia National Laboratories' Extended Probabilistic Risk Assessment Workshop, August 2017
[11] Youngblood, Bob, "Application of Traditional Risk Assessment Methods to Identification of Cyber Manipulation Areas," Idaho National Laboratory, Presented at 2017 Sandia National Laboratories' Extended Probabilistic Risk Assessment Workshop, August 2017
[12] Williams, Adam D., "Intermediate Results from a System Theoretic Framework for Mitigating Complex Risks in International Transport of Spent Nuclear Fuel," Sandia National Laboratories, Presented at 2017 Sandia National Laboratories' Extended Probabilistic Risk Assessment Workshop, August 2017
[13] A. D. Williams, 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, "System Theoretic Frameworks for Mitigating Risk Complexity in the Nuclear Fuel Cycle: FINAL REPORT (SAND2017-TBD)," Sandia National Laboratories, Albuquerque, NM, 2017.
[14] 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

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.[15] 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.

5. KEY CHALLENGES AND TAKEAWAYS

Here we list some of the key concepts, challenges and takeaways from the workshop.

5.1. Key Challenges

3SR Metric Integration

Fundamentally to integrate 3S, metric must be used to translate between safety and security. Creating of these metrics intrinsically necessitates a value judgement between safety and security. It is generally agreed that this should be easily understood and explicitly provided to the decision maker. 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

Many techniques, especially ones relying on qualitative methods required to capture more subjective metrics, result in 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. If we have nothing to anchor such results, how can we make financial decisions to address risk?

Security Assessment Tools

As noted elsewhere, security risk assessment lags safety by several decades. Using safety risk assessment tools for security has quickly faced challenges historically. 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

Because of several of the challenges noted above, a fundamental question remains. Is it 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? Will it ever be possible to understand safety and security tradeoffs objectively, or will risk informed approaches naturally incorporate safety and security separately in the larger deliberative decision making process?

[15] 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

Risk Perception

Key in analyzing risk is the difference in public perception and objectively measured risk assessments. For example, nuclear power is held at much higher standards than other industries. Also, as noted elsewhere, 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.

5.2. Key Takeaways

Security PRAs lack of maturity.

Security PRA's lag 20 years behind safety PRAs, we don't have as mature an understanding of security risk in the community, how do we reconcile this and 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

Although traditionally PRAs have been used to implement additional requirements, the sign of maturity for this field may be in understanding and justifying measures that don't contribute significantly to safety and security. With new methods, we need to constantly ask ourselves: What result does this change from my traditional PRA? What requirement do I no longer need?

Begin by Emphasize similarities between safety and security.

As a starting point for integration of safety and security, we should begin by leveraging similarities first, then we can move into integrating differences. The security benefits of passive cooling and containment of new nuclear reactors is a perfect place to start[14].

Cyber Touches Everything

Cyber risk cannot be thought of in isolation, it touches safety, security and safeguards. In this way, cyber can be thought of as the first regime in which safety and security must be integrated by necessity. Any analysis that looks at cybersecurity in isolation may miss key safety aspects. Since cyber forces us to integrate safety and security, it may be an entry point to understand how to integrate more traditional analysis[7,12].

Cyber Complexity Mimics Safety and Security Complexity

Cyber issues are notoriously complex to understand. When analyzing cyber, it quickly becomes unwieldly and combinatorics makes traditional fault tree analysis unsustainable. This complexity mimics the complexity of analysis that integrate safety and security. Therefore the new concepts, tools, and techniques that are required for cyber may also be required when integrating safety and security.

Success Paths

Success paths, which can be thought of, roughly as the opposite of fault trees, are a useful tool to quickly understand potential safety/security containment requirements. Success paths, or similar concepts arose several times by various speakers as a useful tool to address the above issues of increased complexity of modern analysis.

Culture and Sociological Issues

With and acknowledgement that the audience was largely technical, we must understand many issues are cultural and sociological in nature. As we look to safety and security integration, new cultural and sociological issues may arise that trump technical concerns. We must constantly acknowledge this and work to address these issues as best we can as scientists.

6. PATHS FORWARD AND NEXT STEPS

Here we conclude and review the suggested possible next steps from the workshop breakout sessions and divide the suggestions into short, mid and long term.

6.1. Short Term (0-3 months)

Coordinate a core technical team

Formulate a technical team from across the lab of colleagues that would be interested in contributing 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.

Literature Review

The bulk of the effort in the short term would be a survey of ALL risk-related analysis techniques, approaches and tools throughout the complex (and sample those from beyond). It would be a wide survey of conceptual approaches to risk, starting with[16]. Most of this literature is adversarial modeling, but we would have to widen range to include integration methods.

Identify Customer Need

Identify potential customers, needs, metrics that would be useful. Have potential customers review the ideas and any initial products.

Technical Roadmap

Develop insights from FY17 white paper into 'formal technical' roadmap. This will guide the group and serve as a project plan.

6.2. Medium Term (3-6 months)

Hold an Additional "Working" Workshop

Select 2-3 approaches to test for integrated risk assessment from the literature. as this goes forward, we should include member of the ASME & ANS formed Joint Committee on Nuclear Risk Management (JCNRM).

Work Through One Example

As a follow-on from the 'working' workshop, identify a manageable set of scenarios on which to evaluate risk from 'integrated' perspective. Ideas: Vital area identification. Use fault trees to ID cut set. Technical team may address key needs and issues listed in this workshop.

[16] A. D. Williams, M. DeMenno and A. Macherla, "Exploring Risk Complexity: A Risk Literature Survey & Review (SAND2017-TBD)," Sandia National Laboratories, Albuquerque, NM, 2017.

6.3. Long Term

Evaluation of Scenario Work

The technical team may lead and evaluation of the scenario example from above. Conduct another inter-lab workshop to discuss results and do peer review. Course correct and plot further action based on results.

APPENDIX A: REFERENCES

The material in this report was drawn from the presentations made during the workshop as well as from the facilitated discussions between workshop attendees and organizers. The following is a list of the presentations made.

Presenter	Presentation Title
Apostalakis, George	Historical Perspectives and Current Issues
Brown, Nathanael	A Stochastic Programming Approach to the Design Optimization of Layered Physical Protections Systems
Clark-Ginsberg, Aaron	Assessing Electric Grid Cybersecurity Risks: Three Ideas from Disaster Sociology
Grabaskas, Dave	Advanced Reactor PRA Analytics
Muhlheim, Michael	I&C System Design and Cyber-Security Safeguards
Peterson, Per	PRA Synergies in Safety, Security, and Safeguards
Unwin, Steve	A Threat Methodology: Application to Emerging Technologies
Williams, Adam	Intermediate Results from a System-Theoretic Framework for Mitigating Complex Risks in International Transport of Spent Nuclear Fuel
Wyss, Gregory	Survey of Security Risk Assessment Examples
Wyss, Gregory	Risk Assessment vs. Risk Management
Youngblood, Bob	Application of Traditional Risk Assessment Methods to Identification of Cyber Manipulation Areas

APPENDIX B: WORKSHOP ATTENDEES

Attendee	Affiliation
Apostalakis, George	
Brown, Nathanael	Sandia National Laboratories
Clark-Ginsberg, Aaron	Stanford University, Center for International Security and Cooperation
Dennis, Matthew	Sandia National Laboratories
Dockery, Holly	Sandia National Laboratories
Forrest, Robert	Sandia National Laboratories
Grabaskas, Dave	Argonne National Laboratory
Hsu, Wen	Sandia National Laboratories
McCrory, F. Mitch	Sandia National Laboratories
Muhlheim, Michael	Oak Ridge National Laboratory
Peterson, Per	University of California Berkeley, Department of Nuclear Engineering
Sutton, Katherine	Sandia National Laboratories
Unwin, Steve	Pacific Northwest National Laboratory
Wheeler, Timothy	Sandia National Laboratories
Williams, Adam	Sandia National Laboratories
Wyss, Gregory	Sandia National Laboratories
Youngblood, Bob	Idaho National Laboratory


Sandia National Laboratories