This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2018-7445C

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

PRESENTED BY

Robert Forrest, Jason Reinhardt, Timothy Wheeler, ***Adam D. Williams***,

59th Annual Meeting of the Institute for Nuclear Materials Management

22-26 July 2018

SAND2018-xxxx C. Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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.

Outline

- Introduction
- Historical Approaches & Current Challenges
- Modern Approaches
- Conclusions
  - Challenges
  - Takeaways & Questions
  - Potential Next Steps

Introduction (1/2)

Complexity of nuclear power plants (NPP) necessitated new mechanisms for ***identifying, measuring and assessing the risk of undesired events***

The ***general agreement of a framework*** for considering these safety risks allowed for an improved ability to manage nuclear power

Safety-focused approaches struggle to adequately include:

- ***Malicious, deliberate acts*** (e.g., terrorist acts or protestors)
- ***Non-proliferation issues*** (e.g., nuclear material diversion)

Introduction (2/2)

Treating safety, security, and safeguards concerns independently

- ***At best***, may not take explicit advantage of measures that provide benefits against multiple risk domains
- ***At worst***, it may lead to implementations that increase overall risk due to incompatibilities

An ideal future would have a ***unified analysis framework*** to inform decision making processes and ***to understand overall risks across the domains*** of safety, security, and safeguards

- A so-called ***"extended probabilistic risk analysis" framework, or ePRA***
- Need an integrated safety, security and safeguards risk (or "3SR") framework

Sandia National Laboratories-hosted the Workshop on Extended Probabilistic Risk Assessment (ePRA) in 2017 ***initiate this conversation*** to begin moving towards a 3SR approach

Historical Approaches & Current Challenges (1/2)

Wide acceptance of PRA a result of evolution & maturation of the technique

- Core assumptions/logic still largely in place

Various current attempts at shifting the logical arguments/ focus of risk assessment

- Need to clearly address the implicit & explicit assumptions made when choosing an approach

No one approach is “correct” in any absolute sense

- Each approach has benefits & drawbacks.

Historical Approaches & Current Challenges (2/3)

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

Historical Approaches & Current Challenges (3/3)

Current challenges to developing a 3SR risk management framework:

- ***Inequality*** between PRA for safety vs. PRA for security
- Difficulties relating to adversary modeling
  - They are ***not independent***, therefore ***high*** uncertainty
- Movement from ***analog to digital*** components increases complexity
- Lack of ***well-defined, measureable & actionable*** metrics
- Adequately addressing ***social or cultural issues/influences***

Modern Approaches (1/2)

A 3SR risk management framework can be:

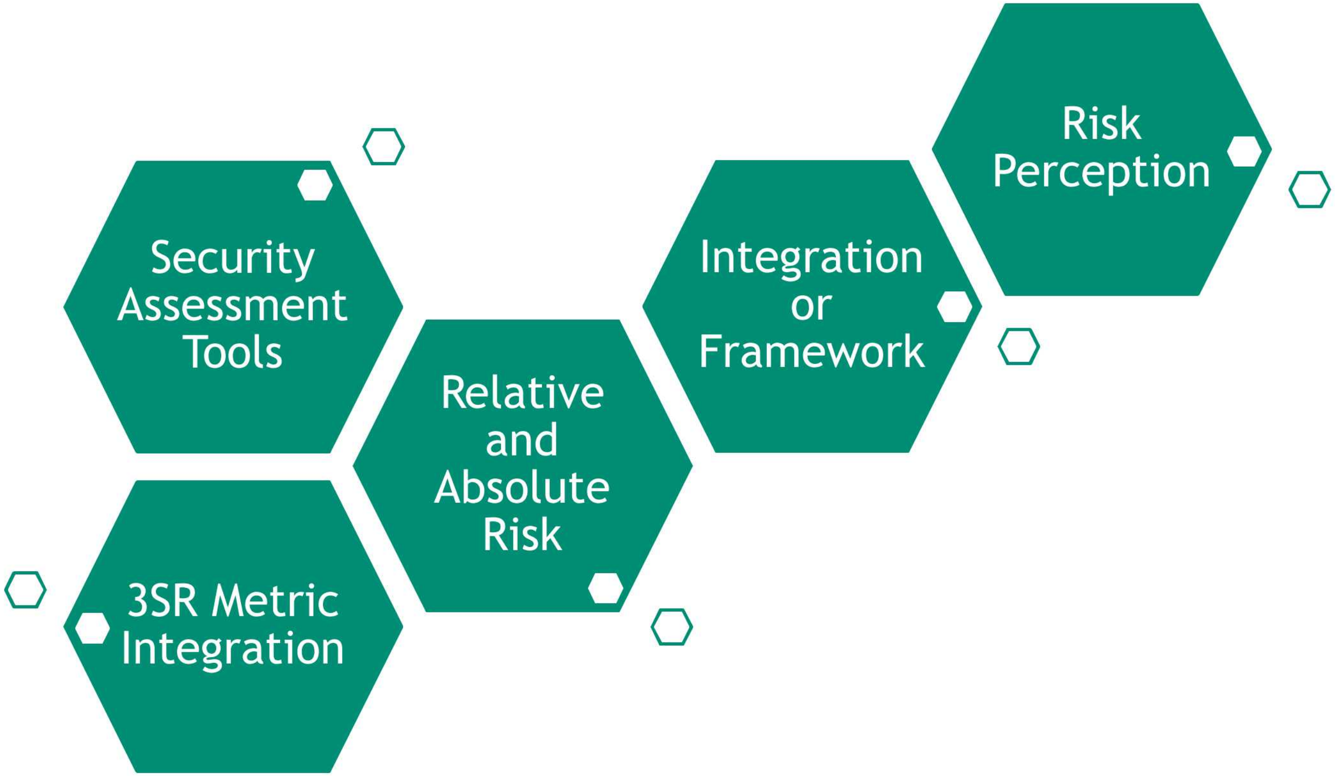
- Informed by the current suite of risk-related analysis towards ***incremental*** improvements
- Guided by identifying ***conflicts and synergies*** between safety & security analyses
- Enhanced by ***understanding the complex interdependencies*** between safety & security risks

Modern Approaches (2/2)

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
Predictive Risk	Methodologies intended to model an adversary's preferred choice of action based on a ***"strategy tree" and a consumer selection model***
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
Optimization Methods	Approaches aimed to ***align the efficiency and effectiveness*** of designing and deploying risk mitigating measures for safety and security
Cybersecurity Assessments	Currently ***borrow the philosophy and application of defense in depth*** strategies to protect critical cyber systems
Integrating Safety & Security Risk Assessments	Recent efforts that have attempted to integrate safety and security risk assessments that ***concluded that such techniques better incorporate multi-faceted interactions in risk analysis***

Conclusions: Challenges

Workshop participants noted a range of ***challenges*** to addressing this problem:



Security Assessment Tools

3SR Metric Integration

Relative and Absolute Risk

Integration or Framework

Risk Perception

Conclusions: Key Takeaways & Questions

Workshop participants several ***takeways/key questions*** for continuing this conversation:

Security PRAs lack of maturity

Utility Comes in Understanding What You Don’t Need

Begin by Emphasizing Similarities between Safety and Security

Cyber Touches Everything

Cyber Complexity Mimics Safety and Security Complexity

Success Paths

Culture and Sociological Issues

Conclusions: Potential Next Steps

Workshop participants noted a ***range of potential next steps*** to move this line of thinking forward:

Short term **(0-3 months):**

- Coordinate a core technical team
- Complete a literature review/risk survey
- Identify customer need(s)
- Develop a technical roadmap

Medium term **(3-6 months):**

- Holding an additional "working" workshop
- Work through an example

Long term **(6+ months):**

- Evaluating scenario work

QUESTIONS?