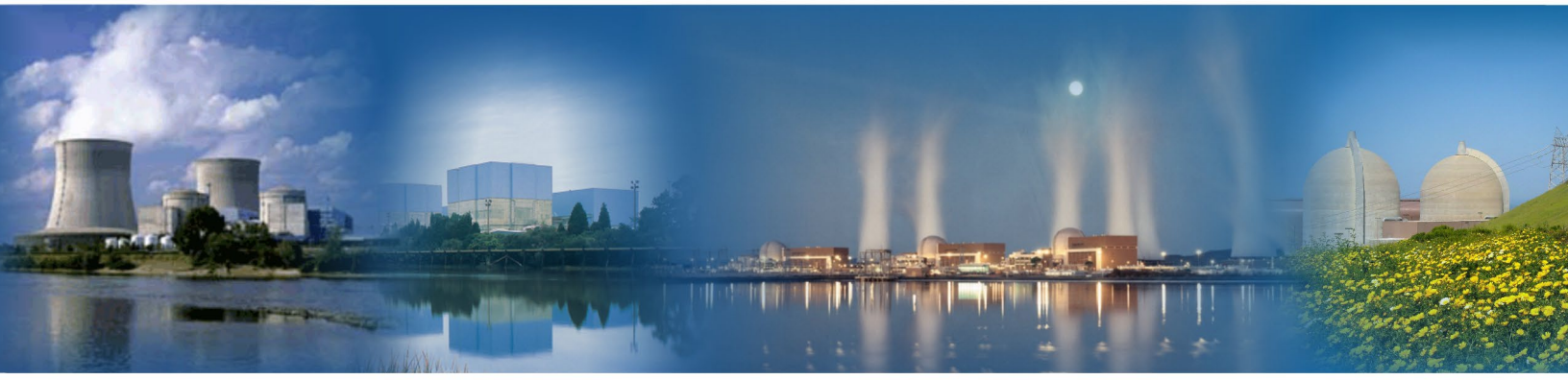
SAND2025-10292R

Light Water Reactor Sustainability Program

Advancing Nuclear Security: A Risk Quantification Methodology



AUGUST 2025

U.S. Department of Energy
Office of Nuclear Energy

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

Prepared by Sandia National Laboratories, Albuquerque, New Mexico 87185

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.

SAND2025-10292R

Advancing Nuclear Security: A Risk Quantification Methodology

Brenton M. Pickrell, Mirvat Abdelhaq, Lon Dawson, Jenna DeCastro, Benjamin Medley*, Matthew Talbot‡

*Contractor with Cogent Security Consulting LLC
‡Contractor with RhinoCorps Ltd

Light Water Reactor Sustainability Program

August 2025

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy

EXECUTIVE SUMMARY

The U.S. Nuclear Regulatory Commission (NRC) plays a vital role in ensuring the safety and security of the United States' commercial nuclear power industry, and has historically maintained high standards of safety and security. In keeping with this legacy, the NRC has been consistently moving toward risk-based strategies in defining security risks[10][11][12]; this document provides the next step.

To address current challenges and to assist in establishing a technical basis for the next step, this paper proposes a risk quantification methodology centered on the concept of "Probability of System Effectiveness" (P_E), and based upon the U.S. Department of Energy's Vulnerability Assessment process[9]. P_E is a quantitative metric representing the likelihood that a PPS will successfully detect, delay, respond to, interrupt, and neutralize an adversary before they achieve their objectives. P_E provides a consistent, repeatable, and scalable framework for evaluating security risk. This methodology empowers licensees to optimize their PPS while maintaining compliance with NRC standards, offering a more agile and efficient pathway for security planning.

The proposed methodology is designed to be optional, allowing utilities to choose whether to adopt it or continue using the current compliance-based system. This flexibility ensures the methodology is adaptable to the diverse needs and financial constraints of individual facilities. For those who opt to transition, the methodology provides benefits such as increased flexibility in security planning, cost optimization, improved decision-making, and adaptability to evolving threats.

For the NRC, the methodology streamlines regulatory processes, reduces administrative burdens, and enhances consistency across the fleet. By providing a quantifiable framework for security risk assessments, the NRC can prioritize resources more effectively, aligning oversight with broader national priorities such as energy independence, technological innovation, and economic resilience. The methodology also supports innovation in nuclear security practices, fostering the use of advanced tools like modeling and simulation programs to enhance statistical reliability and confidence in security planning.

The feasibility and scalability of the methodology were demonstrated through a pilot study at the Monticello Nuclear Generating Plant. The study evaluated guard-force neutralization capabilities and calculated P_E values for adversary scenarios, providing a compelling case for integrating risk quantification methodologies into security planning, and establishing the technical rigor for adoption across the industry. By offering a consistent, repeatable, and scalable framework for evaluating PPS effectiveness, the PE methodology represents a significant step forward in modernizing the regulatory approach to nuclear security.

Through phased integration and alignment with established industry practices, the proposed methodology can be implemented effectively, ensuring stakeholders build confidence in its processes and outcomes. By addressing longstanding challenges and offering a flexible, efficient, and risk-informed framework, the methodology represents a forward-looking approach to nuclear security. Its adoption ensures the nuclear industry remains safe, reliable, and resilient in the face of evolving threats.

This work was conducted as fulfillment to an individual milestone requirement under the Light Water Reactor Sustainability (LWRS) program. This study satisfies M3LW-25SN1203023, and vastly improves the ability to describe and quantify security at an NRC licensed facility.

ACKNOWLEDGEMENTS

The Light Water Reactor Sustainability (LWRS) Physical Security Pathway would like to express our deepest gratitude to the individuals and organizations whose expertise, collaboration, and support were instrumental in the development of this document and the associated study.

Special thanks to Ben Medley at Cogent Security for his invaluable expertise on the Vulnerability Assessment process, consulting on all aspects of the methodology, and writing the initial draft of this document. His contributions provided a strong foundation for this effort and were critical to its success.

We also extend our sincere appreciation to Matt Talbot and Dan McCorquodale at RhinoCorps for their exceptional modeling and simulation expertise. Their consultation and technical insights were vital in leveraging advanced tools and methodologies to evaluate physical protection systems effectively.

This effort would not have been possible without the partnership of Xcel Energy Corporation, and especially Kurt Gosney. Xcel's continuous collaboration and support, as well as their willingness to provide the underlying facility model for this study was essential to its success. Furthermore, their continuous support for the LWRS program has made lasting impacts on the nuclear power industry, driving innovation and progress in ways that benefit the entire sector.

To all contributors, collaborators, and supporters, we extend our heartfelt thanks for your dedication and commitment to advancing nuclear security and resilience, and ensuring the long-term contribution of the nuclear sector to our national security and energy independence.

TABLE OF CONTENTS

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
CDP	Critical Detection Point
CFR	Code of Federal Regulations
DBT	Design Basis Threat
DOE	[U.S.] Department of Energy
FoF	force-on-force exercise
INL	Idaho National Laboratory
LSPT	Limited Scope Performance Test
LWRS	Light Water Reactor Sustainability [Program]
NE	Nuclear Energy
NNSA	National Nuclear Security Administration
NPP	Nuclear Power Plant
NRC	[U.S.] Nuclear Regulatory Commission
P_D	Probability of Detection
P_E	Probability of System Effectiveness
P_I	Probability of Interruption
P_N	Probability of Neutralization
PPS	Physical Protection System
PSP	[LWRS] Physical Security Pathway
ROWS	Remotely Operated Weapons System
SNL	Sandia National Laboratories
VAR	Vulnerability Assessment Report

1. INTRODUCTION

The U.S. Nuclear Regulatory Commission (NRC) plays a critical role in ensuring the safety and security of the United States' commercial nuclear power industry. As the regulator for all domestic non-government reactors, the NRC has upheld a legacy of exceptional safety and security since its founding in 1975. However, there has been recent bipartisan effort to introduce a focus on efficiency, which stems largely from an acknowledgement that safe, inexpensive, clean, abundant energy is critical to national security. The historically prescriptive nature of many NRC regulations runs counter to this effort, and while effective in maintaining baseline protections, these regulations have introduced challenges that impact the flexibility and adaptability of licensees in addressing modern threats and optimizing resources.

A novel approach to security planning, grounded in risk quantification and based upon the NNSA Vulnerability Assessment process[9], offers a promising pathway to address these challenges. By establishing a quantifiable "Probability of System Effectiveness" (P_E) against the Design Basis Threat (DBT), this methodology provides licensees with a framework to evaluate and modify their security plans while maintaining compliance with NRC standards. Unlike the current prescriptive process outlined in 10 CFR § 50.54(p)[6], which limits flexibility and can discourage voluntary enhancements by enforcing the achieved level of security or higher in perpetuity, this approach offers a more agile and efficient pathway for security planning.

The adoption of such a methodology also aligns with broader efforts to increase efficiency and reduce unnecessary burdens within the NRC, by alleviating a significant workload associated with evaluating change requests and license amendment actions. Also, this ensures industry can adapt to evolving challenges while continuing to provide inexpensive, reliable, and abundant energy. By empowering licensees to optimize their security apparatus, this approach supports and synchronizes the goals of enhancing operational efficiency and maintaining robust protections against potential threats.

1.1. Background

The regulatory framework governing the United States' commercial nuclear power industry has been shaped by decades of commitment to safety and security. Since its establishment in 1975, the NRC has played a pivotal role in ensuring the safe operation of domestic non-government reactors. This framework has successfully maintained a high standard of safety and security, but has also introduced prescriptive requirements that can limit flexibility and adaptability in addressing evolving threats and optimizing security resources.

One of the most significant regulatory challenges faced by licensees is embedded in 10 CFR § 50.54(p)[6], which mandates that any changes to physical security plans, guard training and qualification plans, or cybersecurity plans must not decrease the effectiveness of those plans. While this requirement ensures robust security, it has led to what is commonly referred to as the "ratcheting effect." This phenomenon occurs when voluntary security enhancements, even those not required by regulation, become permanent obligations. If such enhancements fail or become unsustainable, licensees are required to restore the security apparatus to the level of effectiveness provided by all previous enhancements, often at significant financial cost. This creates a scenario where licensees are effectively discouraged from implementing voluntary improvements by fear of future obligations, which stifles innovation and adaptability in security planning.

Recent legislative and executive actions have sought to address these challenges by emphasizing efficiency, flexibility, and modernization within the nuclear regulatory framework. The ADVANCE Act[5] of 2024, signed into law by President Biden, represents a bipartisan effort to accelerate the deployment of advanced nuclear technologies and reduce regulatory barriers. Among its provisions, the Act calls for streamlined licensing processes, reduced fees, and incentives for innovation, reflecting a broader recognition of the critical role nuclear energy plays in achieving energy independence and national security.

In addition to legislative efforts, President Trump has issued multiple Executive Orders aimed at cultivating nuclear power expansion, enhancing the fiscal viability of nuclear power production efforts to encourage growth, and supporting other applications for nuclear power in an effort to bolster national security. Executive Order 14300 (Ordering the Reform of the Nuclear Regulatory Commission)[1] highlights the need for the NRC to balance safety considerations with the benefits of increased availability and innovation in nuclear power. It calls for fixed deadlines in licensing processes, science-based radiation limits, and streamlined public hearings, among other reforms. Similarly, Executive Order 14302 (Reinvigorating the Nuclear Industrial Base)[2] underscores the importance of strengthening the domestic nuclear fuel cycle, restarting closed nuclear plants, uprating current plants, constructing new nuclear production facilities, and preparing the workforce to support the expansion of nuclear energy. These directives align with broader national priorities, including those outlined in Executive Order 14156 (Declaring a National Energy Emergency)[4] and Executive Order 14262 (Strengthening the Reliability and Security of the United States Electric Grid)[3], which emphasize the critical role of energy security and resilience in supporting technological innovation, economic prosperity, and national defense.

The DBT serves as a cornerstone of the NRC's security framework, providing a standardized adversary model against which each licensee's security apparatus is evaluated. For example, the DBT specifies the number of adversary and likely adversary characteristics, ensuring security plans are tailored to credible threats. Given that the DBT is the set of adversary characteristics against which security is measured at all NRC licensed sites, care should be taken to ensure it is well aligned with similar estimates across other government agencies and departments.

The proposed risk quantification methodology, which introduces the concept of P_E, offers a promising solution to these challenges. By establishing a quantifiable lower limit for P_E against the DBT, this methodology would provide licensees with an option for evaluating and modifying their security plans, which is focused around effects. This approach aligns with the broader goals of recent legislative and executive actions, ensuring that the nuclear industry remains a cornerstone of America's energy security and economic prosperity.

1.2. Motivation

The nuclear power industry is at a critical juncture, where the need for safe, reliable, and cost-effective energy must be balanced against evolving security challenges, regulatory compliance, and economic viability. As the United States seeks to expand its nuclear energy capacity to meet growing electricity demand, support advanced technologies, and bolster national security, it is imperative to garner efficiencies wherever possible. The NRC is adapting to the requirements prescribed in the ADVANCE Act, Executive Orders and other guidance they have received in an agile and responsive manner. This framework is intended to further assist in those efforts.

One of the most pressing challenges is the rigidity of 10 CFR § 50.54(p), which requires licensees to maintain or exceed the effectiveness of their security plans with every modification. While this mandate ensures robust protections, it has created a "ratcheting effect" that discourages voluntary security enhancements. Licensees are often hesitant to implement improvements, knowing that even optional upgrades will become permanent obligations, potentially leading to significant financial and operational burdens in the future. This dynamic stifles innovation, limits adaptability, and prevents licensees from optimizing their security apparatus to address modern threats effectively, often waiting until a requirement is published that mandates their action.

The proposed risk quantification methodology, centered on the concept of P_E, directly addresses these challenges by introducing a quantifiable and repeatable framework for security planning. By establishing a lower limit for P_E against the DBT, this methodology provides licensees with the flexibility to evaluate and modify security plans using a more agile justification under the 10 CFR § 50.54(p) process. This approach empowers licensees to make agile, cost-effective decisions while maintaining compliance with NRC standards and ensuring robust protections against credible threats.

The motivation for adopting this methodology extends beyond the operational benefits for licensees. For the NRC, the current process for evaluating changes under 10 CFR § 50.54(p) and license amendment actions under 10 CFR § 50.90, represents a significant workload, which requires extensive resources to review and approve modifications. By offering an optional framework based on P_E, the NRC can streamline its regulatory processes, reduce administrative burdens, and focus its resources on higher-priority issues. This aligns with recent legislative and executive directives, such as the ADVANCE Act of 2024 and Executive Order 14300, which emphasize efficiency, modernization, and the reduction of unnecessary regulatory barriers.

Moreover, the adoption of such an approach supports broader national priorities, including energy independence, technological innovation, and economic resilience. Nuclear power is uniquely positioned to provide clean, inexpensive, reliable, and abundant energy, which is critical for powering advanced industries such as artificial intelligence, quantum computing, and domestic manufacturing. As highlighted in Executive Order 14156 (Declaring a National Energy Emergency) and Executive Order 14262 (Strengthening the Reliability and Security of the United States Electric Grid), the integrity and resilience of the energy infrastructure are vital to national security and economic prosperity. By enabling the nuclear industry to adapt more efficiently to evolving challenges, the proposed methodology ensures that nuclear power remains a cornerstone of America's energy strategy.

The motivation for this methodology also stems from the recognition that modern threats require modern solutions, but the current regulatory framework limits the ability of licensees to address emerging risks effectively. A framework focused on P_E allows licensees to tailor their security plans to specific threats, ensuring that resources are allocated efficiently and that protections remain robust in the face of evolving adversary capabilities.

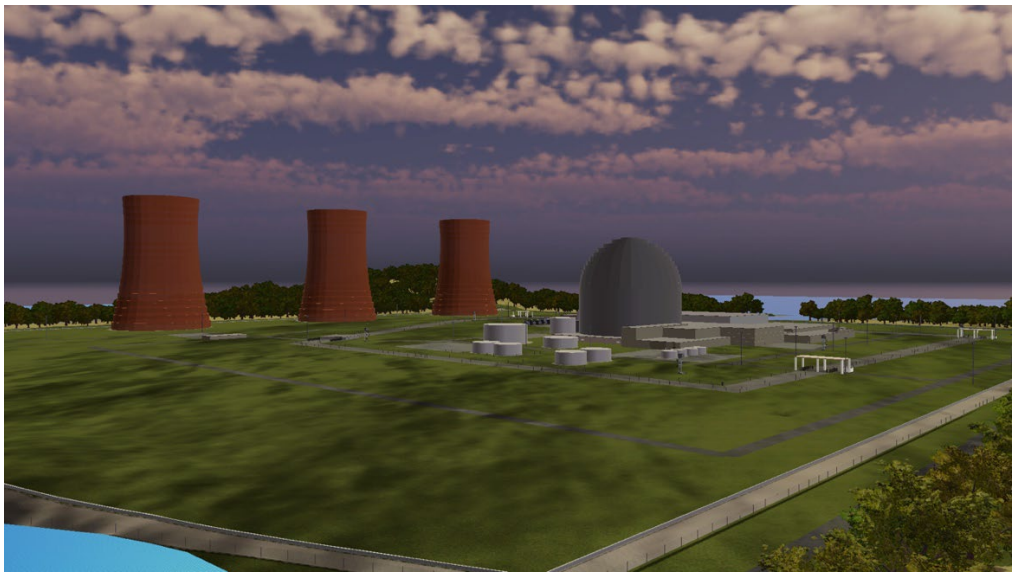
In summary, the proposed risk quantification methodology is motivated by the need to enhance flexibility, efficiency, and innovation within the nuclear regulatory framework. By empowering licensees to optimize their security apparatus and alleviating some administrative burdens on the NRC, this approach supports the dual goals of operational excellence and regulatory modernization. Furthermore, it aligns with national priorities to ensure that nuclear power continues to play a pivotal role in America's energy future, technological leadership, and national security.

2. PILOT STUDY: MONTICELLO NUCLEAR GENERATING PLANT

In June 2025, RhinoCorps LLC, under contract to Sandia National Laboratories, completed a pilot study to evaluate guard-force neutralization capabilities at the Monticello Nuclear Generating Plant. This study leveraged advanced modeling and simulation tools to provide quantitative insights into the effectiveness of the plant's physical protection system (PPS). Using the Simajin® Application Suite, RhinoCorps created a detailed facility model based on data provided by the licensee, Xcel Energy, and evaluated adversary attack scenarios to calculate key security metrics. The study represents a significant step toward integrating quantifiable methodologies into nuclear security planning, offering a scalable framework for risk-informed decision-making.

It is important to note, that while this study utilized RhinoCorps' Simajin® software, there are other options available. The utilization of one software in this study should not be construed as an endorsement, as there are other such products available that may be equally effective.

Figure 2.1 Example Facility Model



2.1. Scope and Objectives

The primary objective of the pilot study was to assess the guard-force neutralization capabilities at the Monticello Nuclear Generating Plant using an approach that can effectively standardize risk quantification and apply across the industry. Specifically, the study aimed to:

- Develop a detailed facility model using the Simajin® Application Suite, incorporating site-specific data provided by Xcel Energy.
- Evaluate adversary attack scenarios developed by Xcel Energy to calculate the probability of neutralization (P_N) for each scenario.
- Determine the P_E for the PPS.

- Demonstrate the utility of software-based simulations in generating quantitative security metrics to inform risk-informed decision-making.
- Provide insights into the scalability and applicability of the P_E methodology for broader use across the commercial nuclear fleet.

The study focused exclusively on adversary scenarios provided by Xcel Energy, with probability of detection (P_D) values derived from the site's physical and human security components. While the pilot did not address the likelihood or consequence of an attack, it provided a foundational framework for evaluating security risk based on PPS effectiveness.

2.2. Methodology

The pilot study employed the Simajin® Application Suite, a software tool designed to simulate force-on-force (FoF) engagements in a batch format. Modeling and simulation programs like Simajin® are essential tools for evaluating complex systems, such as physical protection systems (PPS), in a controlled and repeatable manner. These programs break down each individual action within a scenario into probabilistic outcomes based on established parameters and behaviors. For example, when an adversary encounters a security worker, the simulation calculates probabilities for key events, such as when each individual notices the other. This probability is influenced by factors such as whether one party is hiding while the other is walking, which increases the likelihood of noticing the other party. From there, the simulation evaluates probabilities for all subsequent actions, such as engagement or non-engagement (e.g., choosing to remain hidden), and if engagement occurs, both timing and probabilities for hit and kill outcomes are calculated for each shot fired. The engagement probability is government-controlled data provided by the U.S. Department of Energy (DOE), while many other supporting data values (e.g. movement speeds, weights of objects, etc.) are standardized to enforce consistency.

This granular approach allows modeling and simulation programs to model complex interactions and decision-making processes with a high degree of statistical reliability. By running hundreds of scenarios with varying inputs and probabilities, modeling and simulation provides robust datasets that are far more statistically reliable than live FoF exercises alone. Live exercises, while valuable, are limited in the number of runs that can be conducted due to logistical, safety, and cost constraints. In contrast, modeling and simulation enables the evaluation of hundreds (or even thousands) of scenarios, ensuring that results are both repeatable and representative of a wide range of conditions.

Validation is a critical component of the modeling and simulation process. To ensure accuracy, simulations are compared to live FoF exercises conducted under similar conditions. Any notable discrepancies between the simulated and live results are analyzed, and adjustments are made to the model or simulation to improve fidelity. This iterative process ensures that modeling and simulation outputs align closely with real-world outcomes, enhancing confidence in the results and their applicability to security planning.

Most validated modeling and simulation programs enable users to program tactical variations, adversary pathways, and guard-force responses, generating detailed, site specific outputs such as geolocated events, engagement geometry, and character behavior. These outputs are critical for validating the accuracy of the simulations and informing risk-informed decision-making. The ability to simulate hundreds of runs for each scenario, combined with probabilistic modeling of individual actions, makes modeling and simulation an indispensable tool for modern vulnerability assessments.

Figure 2.2 Software-based Neutralization Analysis

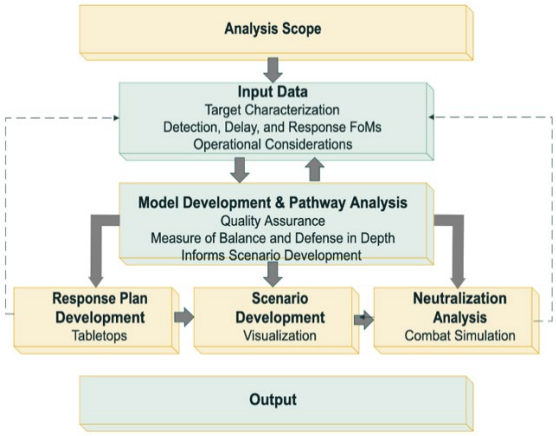


Figure 2.2 illustrates the iterative process of software-based Neutralization Analysis, highlighting how foundational information interacts to inform response planning, scenario development, and neutralization strategies to create an output that enhances risk management.

The methodology included the following key steps:

1. Facility Modeling: RhinoCorps developed a detailed model of the Monticello Nuclear Generating Plant using site-specific data provided by Xcel Energy. This model included both interior and exterior physical infrastructure, terrain, and security system components.
2. Scenario Development: Adversary attack scenarios were created by Xcel Energy, incorporating the DBT and site-specific threat vectors. These scenarios included variations in adversary tactics, pathways, and objectives and were inspired by current and past exercises.
3. Defensive Strategy Modeling: The current (baseline) defensive strategy was provided by Xcel Energy and modeled by RhinoCorps. This defensive strategy models the defensive personnel (including weapons and equipment) as well as pre- and post-alarm actions described in Xcel's defensive strategy procedures.
4. Simulation Runs: Each scenario was tested using 250 simulation runs or until a 95% confidence interval was achieved for guard-force wins. Wins were defined as instances where the adversary failed to complete their objectives.
5. P_N Calculation: P_N was calculated using an industry-standard equation:

Figure 2.3 P_N Calculation

$$P_N = \frac{\text{Wins}}{\text{Tests}} * \left(1 - \frac{1}{2\sqrt{Tests}}\right)$$

This equation provides a 95% confidence level for P_N based on the number of wins and total tests.

6. P_E Calculation: Great care was taken in determining the process by which P_E is calculated, since this is the primary function of the process. The parent process (DOE Vulnerability Assessment) was considered against the needs of NRC licensed facilities, and caution was taken to ensure rigor remained at the appropriate level while adjusting portions of the process to Account for regulatory and facility differences.

P_E was computed using the same formula provided above for P_N, because the characteristics of the system used under the parent process to calculate P_I were fully incorporated into the model. This is termed "the holistic method" which eliminates the need for aggregating the probabilities of various detection values provided by layers in the security system, and replaces that process with a single simulation accounting for these nuances in their totality. Based on the idea that all P_I data is incorporated into the model (all tests include P_I inherently), the P_N above is synonymous with P_E.

Figure 2.3 P_E Calculation Using Holistic Method

$$P_E \cong \frac{Wins}{Tests} \times \left[1 - \left(\frac{1}{2\sqrt{Tests}}\right)\right]$$

If this method is not employed, either by tool limitation or analyst decision, the P_E must include a calculation that incorporates sufficient rigor to compute all detection probabilities from the critical detection point outward to the start of the attack, this is known as probability of interruption (P_I). In this case, PE must then be calculated using the following formula:

Figure 2.4 P_E Calculation Using P_I at CDP

$$P_E = P_N \times P_I$$

7. Analysis and Reporting: Results were analyzed to identify key insights into PPS effectiveness, including areas for potential improvement. Visual reporting tools, such as death plots, were used to validate the scenarios and ensure the accuracy of the simulations.

2.3. Findings

While the pilot study results include site specific, proprietary and safeguards information that cannot be widely released, the effort yielded several key findings that highlight the utility of this or similar methodologies in nuclear security planning:

1. Quantitative Security Metrics: The study successfully calculated P_N and P_E values for each evaluated scenario, providing a repeatable and consistent framework for assessing PPS effectiveness. These metrics offer a more nuanced understanding of security risk compared to traditional compliance-based approaches.
2. Utility of Software-Based Simulations: This use of modeling and simulation software demonstrated its value in evaluating PPS effectiveness. Simulations provided insights into adversary and guard-force interactions that would be difficult or unsafe to replicate in real-world FoF exercises. There are multiple competing and similar programs, the fact that Simajin® was used in this study should not be construed as an endorsement for that program.
3. Scenario Validation: Visual reporting tools, such as death plots, were instrumental in validating the scenarios and ensuring the accuracy of the simulations. These tools allowed auditors to review geolocated events, engagement geometry, and character behavior, enhancing confidence in the results.

4. Scalability and Applicability: The pilot study demonstrated the scalability of the P_E methodology for broader use across the commercial nuclear fleet. By leveraging site-specific data and standardized adversary scenarios, the methodology can be adapted to diverse facility configurations and threat environments.
5. Potential for Cost Savings: The proposed approach offers significant potential for cost savings by effectively enabling the site to describe the effects of their security apparatus against a DBT adversary. This reduces regulator effort in evaluating the security of a site, and enables sites to tailor security solutions and optimize resources without compromising effectiveness. This aligns with broader goals to reduce redundancy and enhance operational efficiency.
6. Rapid Adjustment or Iteration: This approach allows evaluation of multiple possibilities with a comparison between each. The statistical and probabilistic outcomes create a rationale for use of employing certain strategies over others, and allow iteration for cost saving purposes.

The findings from the Monticello pilot study provide a compelling case for integrating risk quantification methodologies into security planning. By offering a consistent, repeatable, and scalable framework for evaluating PPS effectiveness, the P_E methodology represents a significant step forward in modernizing the regulatory approach to nuclear security.

3. PROPOSED RISK QUANTIFICATION METHODOLOGY

The proposed risk quantification methodology introduces a novel approach to security planning, centered on the concept of P_E. P_E is a quantitative metric that represents the likelihood that a physical protection system (PPS) will successfully detect, delay, respond to, interrupt, and neutralize an adversary before they achieve their objectives. Unlike traditional compliance-based approaches, which rely on fixed requirements and prescriptive standards, this methodology focuses on achieving desired outcomes, offering flexibility and adaptability to licensees.

3.1. System Effectiveness with Modeling and Simulation Software

This new approach to computing system effectiveness is the recommended approach for NRC licensees employing modeling and simulation tools. The parent methodology's approach for computing "layer-based" P_E, was designed to address previous limitations in computer simulations and computer hardware dating back decades. Advances in computing capabilities and full combat simulation software tools have moved past those original limitations and now allow for the employment of a "holistic" approach.

The holistic approach models detection capabilities as they exist within the facility model to compute neutralization, with the corresponding probabilities of detection for each of those systems or processes. Unlike in the layer-based process, where detection at the layer being analyzed is always assumed, detection is not assumed at any security layer, and as the adversary traverses layers and each intrusion detection system, a detection chance is drawn and compared to the detection probability in the facility model, to determine if the detection occurs for that individual simulation execution. If the adversary is undetected, then they may proceed along their route of travel, attempting to maintain a stealthy posture as appropriate for the scenario.

The benefits of implementing the holistic method include a more natural evolution of the scenario as expected by the adversary and the defense. This process also reduces the total number of simulations required to a third of those required by a three-layer analysis, may reduce the number of scenario variations needed to allow the adversary to progress to the layer being analyzed without detection and removes the need to compute the probability of detection at each layer. However, it requires the analyst and tool to include more data in the models to represent the detection probabilities identified in the facility characterization and documentation process.

This methodology allows licensees to evaluate their PPS against the DBT, and compare various strategies. By establishing a quantifiable lower limit for P_E using this framework, the NRC can define an acceptable threshold for security effectiveness, enabling licensees to make changes to their security plans as long as they remain above the accepted threshold. This approach provides a consistent, repeatable, and scalable framework for assessing security risk, empowering licensees to optimize their PPS while maintaining compliance with NRC standards.

3.2. System Effectiveness Using Exercises as Supporting Data

For cases where fewer than 33 data points are available, the following equation is used to compute P_N. This equation will allow sites to compute a P_N value if they choose to simply use existing LSPT and FoF methods.

$$P_N \cong \frac{Wins + 0.5}{Tests + 1.0}$$

However, for these cases, P_D has not been considered within the framework as it was in the holistic method, meaning P_D must be included in the calculation as mentioned above. The probability of detection for each layer, or each security sensor an adversary encounters must be aggregated, which provides a comprehensive P_D. This may be accomplished by using the following formula:

$$P_D = 1 - \left(1 - P_{D(Layer\ 1)}\right) \times \left(1 - P_{D(Layer\ 2)}\right) \times \ldots \left(1 - P_{D(Layer\ n)}\right)$$

Thus, when using fewer than 33 data points, the P_E for each baseline scenario will be multiplied by the detection probability calculated above. This PD value will be less than 1.0 in all cases. Detection probabilities must consider the possibility of a failure to properly identify the initiation of the attack. For example, even initiating an explosive breaching charge within easy hearing of guard force members may realistically result in misidentification of the source of the sound, and thereby result in the initiation of the attack not being detected in effect.

$$P_E \cong P_D * \frac{Wins + 0.5}{Tests + 1.0}$$

3.3. Implementation Framework

The implementation of the proposed methodology requires a structured framework that integrates the proposed evaluations into the existing regulatory processes. The following steps outline the pathway for adoption:

1. Establishing the Lower Limit for P_E: The NRC would define a minimum acceptable P_E threshold based on risk-informed principles against the DBT. This threshold would serve as the baseline for evaluating security effectiveness at participating licensed facilities. It is important to note that the mathematical framework described above should play a central role in determining this limit. For instance, when calculating P_E using a holistic method, even a perfect 250 wins out of 250 modeling and simulation runs yields a P_E of only 96.8%. This demonstrates that the formula inherently incorporates conservatism, and adding further conservatism to the threshold would risk perpetuating the current challenges faced by licensees. Careful consideration is therefore required to ensure the lower limit is both realistic and achievable.

2. Developing Standardized Scenario Suites: The NRC would consider the most likely and most consequential threats facing all licensed facilities (e.g. active shooter, precision engagement, etc.) and provide a list of these threats. As a note, these threats should be broad and apply universally (or nearly so, with possible exclusions) to licensees. Licensees would then create specific adversary scenarios aligned with each item on this threat listing, and tailored to their site-specific characteristics, including terrain, infrastructure, and local threat environment.

3. Calculating P_E at the Site: The P_E must be calculated at each location using one of the two methods outlined above. First, that may be done by adopting validated modeling and simulation tools, which are capable of calculating the P_E based on the holistic method. Alternatively, licensees may utilize exercises and P_D for system components as supporting data to establish P_E with the formulas outlined above.

4. Integrating Quantification Evaluations: Licensees would use the P_E methodology to better describe the performance of their security apparatus as a whole. As long as the calculated P_E remains above the established threshold, sites would have the agility to make changes without requiring extensive NRC review under 10 CFR § 50.54(p)[6], and the NRC would have a common universally applicable construct to enable comparisons and ensure adequate security across the whole of industry.

5. Phased Integration: The methodology would be introduced through a phased approach, starting with pilot studies at select facilities. Lessons learned from these pilots would inform broader adoption across the commercial nuclear fleet.

6. Regulatory Oversight: The NRC would maintain oversight through periodic audits and inspections, ensuring that licensees adhere to the methodology and that P_E calculations are accurate and reliable.

This framework provides licensees with the flexibility to optimize their security apparatus while reducing the administrative burden on the NRC. By shifting the focus from prescriptive compliance to effects-based outcomes, the methodology aligns with broader efforts to modernize the regulatory framework and enhance efficiency.

3.4. Challenges and Considerations

While the proposed methodology offers significant benefits, its implementation requires careful consideration of several key challenges:

- Analysis Process Considerations: Accurate P_E calculations depend on reliable metrics for detection, delay, and response capabilities. Establishing these metrics requires robust data collection and validation processes, as well as standardized methods for evaluating adversary scenarios. Additionally, an adversary knowledge construct must be developed to define reasonable bounds on what adversaries are assumed to know about a facility's security system.
- Scenario Development: The creation of standardized scenario suites is critical to ensuring consistency and repeatability across the fleet. These scenarios must account for credible threat vectors, such as waterborne attacks or deceit tactics, and include a complexity scoring matrix to balance adversary capabilities across different vectors.
- Tool Validation: Modeling and simulation tools must be rigorously validated through live force-on-force (FoF) exercises to ensure their accuracy and reliability. Discrepancies between simulated and live results must be evaluated and the cause of the discrepancy noted. In the case of the discrepancy being caused by an artificiality in the live exercise, the exercise director should determine corrective measures. In the case of the discrepancy being attributed to the modeling and simulation efforts, this should be addressed through iterative adjustments to the model or simulation, and the simulations run again.
- Regulatory Approval Process: The NRC must establish regulations that minimize delays while maintaining confidence in the results and the security of nuclear facilities.
- Consistency Across Licensees: To avoid inconsistent application of the methodology, the NRC must provide clear guidance on key inputs, assumptions, and evaluation criteria. This

includes defining the threat-vector matrix, adversary knowledge construct, and security system effectiveness metrics.

- Industry Adoption: Licensees may face initial resistance to adopting the methodology using the holistic method due to the perceived complexity of modeling and simulation tools and the need for additional training and resources. Further, model development is often costly (approximately $250,000) and is typically proprietary. This issue should be adequately mitigated by the ability for sites to use exercises, which are already conducted regularly as the justifying data. Further, the NRC should allow flexibility across the fleet for utilities to adopt this methodology, or to continue to rely on the current process and standards.

By addressing these challenges, the proposed methodology can achieve its full potential, providing a flexible, efficient, and risk-informed framework for nuclear security planning.

4. PROPOSED IMPLEMENTATION STRATEGY

The successful adoption of the proposed risk quantification methodology requires a structured and deliberate implementation strategy that balances innovation with practicality while respecting the diverse needs and preferences of individual facilities. Facilities should choose to transition to this quantifiable risk management strategy or continue using the current compliance-based system if they find it more cost-effective or better suited to their operational needs.

By leveraging lessons learned from the pilot study at the Monticello Nuclear Generating Plant and benchmarking against established practices in the nuclear security industry, the implementation strategy aims to provide a scalable framework for integrating quantifiable risk management into NRC processes. The phased approach ensures that facilities adopting the methodology can do so incrementally, minimizing disruptions and allowing for refinements along the way.

4.1. Phased Integration

To facilitate the voluntary adoption of the proposed methodology, the implementation strategy proposes a phased integration process. This approach allows facilities to evaluate the benefits of transitioning to the new system while maintaining the option to continue with the current compliance-based approach. The phases include:

1. Initial Endorsement and Review: The first step involves developing a comprehensive plan for licensee endorsement and NRC review. This plan would document the processes, methods, and steps for licensees to create standardized adversary scenarios and calculate P_E values. It would also define how security risk is consistently determined across the fleet, incorporating essential constructs such as detection, delay, and response metrics. The plan should account for site-specific nuances, such as reactor types and domestic threat environments, while maintaining consistency in evaluation criteria. Licensees would have the option to adopt this plan or continue with the existing system.
2. Pilot Vulnerability Assessment: A pilot study would be conducted at several facilities that voluntarily choose to evaluate the full vulnerability assessment process using the proposed methodology. This pilot would integrate existing prescriptive security requirements, such as target set determinations based on probabilistic risk assessments (PRAs), compliance-based PPS elements, and the NRC DBT. Modeling and simulation tools would be used to calculate P_E values, providing a quantifiable basis for assessing security effectiveness. Lessons learned from the pilot would inform refinements to the methodology and processes.
3. Force on Force Validations and Audits: The NRC should incorporate evaluating this Risk Quantification process into their current evaluation structure, and should compare the outcomes of a witnessed force-on-force exercise to the results of this process.

This phased approach ensures that stakeholders can build confidence in the methodology while addressing challenges and refining processes. It also provides flexibility for licensees to choose the system that best aligns with their operational and financial priorities.

4.2. Alignment with Industry Practices

The proposed methodology aligns closely with established practices in the nuclear security industry, particularly the vulnerability assessment processes employed by the NNSA and DOE. These processes provide a consistent framework for evaluating security risk across diverse facilities, offering

valuable insights for the implementation strategy. Importantly, the voluntary nature of the methodology allows licensees to decide whether these practices are suitable for their specific needs.

- Like the NNSA process, the proposed methodology emphasizes the development of broadly standardized adversary scenarios that account for credible threat vectors. These scenarios are not intended to be standardized at the tactical level; rather, the commonality between sites would be limited to the overarching threat vector utilized in each scenario (e.g., waterborne attacks, deceit tactics, etc.). Individual sites would retain responsibility for defining tactical details, such as adversary pathways, guard-force configurations, and target configurations, to reflect their unique characteristics. This approach provides a consistent framework for evaluating security risk while preserving the flexibility needed to address site-specific nuances. Facilities that choose to adopt the methodology would benefit from these standardized scenarios, while others may continue using their existing processes.
- Quantifiable Risk Metrics: The NNSA process includes the calculation of P_E values for each scenario, which are averaged across a suite of baseline scenarios to determine the overall risk result for each target. Similarly, the proposed methodology uses P_E as a quantifiable metric for assessing PPS effectiveness, ensuring consistency and repeatability in risk assessments. Licensees opting into the methodology would gain access to these metrics, while others may rely on traditional compliance-based evaluations.
- Tool Validation and Integration: The NNSA process requires the use of multiple methods, including software-based simulations and live FoF exercises, to validate security risk assessments. The proposed methodology incorporates similar validation techniques, ensuring that modeling and simulation tools are accurate and reliable. By leveraging validated tools like Simajin® , the methodology provides robust datasets and statistical reliability, enhancing confidence in the results. Facilities that prefer not to invest in modeling and simulation tools can continue using live FoF exercises as their primary evaluation method.
- Vulnerability Assessment Reports: The NNSA process culminates in the creation of vulnerability assessment reports (VARs) that document key findings, figures of merit, scenario details, and system effectiveness conclusions. The proposed methodology would similarly require licensees opting into the system to document their P_E calculations, scenario evaluations, and supporting data, providing transparency and accountability in security planning. Facilities that choose to remain with the current system would continue documenting their compliance-based evaluations.

By aligning with these industry practices, the proposed methodology ensures that it is grounded in proven principles and techniques. The voluntary nature of the methodology allows licensees to evaluate its benefits and determine whether it is the right fit for their facility, ensuring flexibility and choice in security planning.

5. BENEFITS OF THE PROPOSED METHODOLOGY

The proposed risk quantification methodology offers transformative benefits for both NRC licensees and the regulator itself. By introducing a quantifiable framework for evaluating security risk, the methodology empowers licensees to optimize their physical protection systems (PPSs) while maintaining compliance with NRC standards. At the same time, it alleviates administrative burdens on the NRC, enabling the regulator to focus its resources on higher-priority issues. This optional framework provides flexibility for licensees to adopt the methodology if it aligns with their operational and financial priorities, ensuring that the system is adaptable to the diverse needs of the commercial nuclear fleet.

5.1. For NRC Licensees

- Flexibility in Security Planning: The methodology allows licensees to make changes to their security plans as long as they remain above the established lower limit for P_E. This flexibility eliminates the "ratcheting effect" associated with 10 CFR § 50.54(p), enabling licensees to implement voluntary enhancements without fear of future obligations, and allows significant agility in the application of security.
- Cost Optimization: By focusing on quantifiable outcomes rather than prescriptive requirements, the methodology enables licensees to design security systems tailored to their site-specific characteristics. This reduces unnecessary redundancy and allows for more efficient allocation of resources, potentially resulting in significant cost savings.
- Improved Decision-Making: The use of modeling and simulation tools provides robust datasets and statistical reliability, enabling licensees to make informed decisions about their PPS configurations. This data-driven approach enhances confidence in security planning and risk management.
- Adaptability to Evolving Threats: The methodology's focus on quantifiable risk metrics ensures that licensees can adapt their security systems to address emerging threats effectively. By leveraging standardized threat vectors and site-specific tactical details, licensees can maintain robust protections against credible adversary scenarios. Further, the same system could be used to evaluate threats outside the DBT at the site's discretion, if desired.
- Optional Adoption: The voluntary nature of the methodology ensures that licensees can evaluate its benefits and choose whether to adopt it or remain with the current compliance-based system. This flexibility respects the diverse needs and financial constraints of individual facilities.

5.2. For the NRC

- Streamlined Regulatory Processes: The methodology reduces the administrative burden associated with evaluating change requests and license amendment actions. By providing a quantifiable framework for security risk assessments, the NRC can prioritize resources more effectively.
- Consistency Across the Fleet: The use of standardized adversary scenarios and quantifiable P_E metrics ensures consistency and repeatability in security risk assessments. This enables the NRC to compare security effectiveness across diverse facilities, enhancing its ability to manage risk at the fleet level.

- Alignment with National Priorities: The methodology supports broader national goals, such as energy independence, technological innovation, and economic resilience. By empowering the nuclear industry to optimize its security systems, the NRC contributes to the reliability and affordability of nuclear energy as a cornerstone of America's energy strategy.
- Enhanced Regulatory Agility: The quantifiable nature of the methodology allows the NRC to adapt its processes to address evolving challenges and emerging threats. This agility ensures that the regulator remains responsive to the needs of the industry while maintaining robust oversight.
- Support for Innovation: By encouraging the use of advanced tools like modeling and simulation programs, the methodology fosters innovation in nuclear security practices. This aligns with recent legislative and executive directives aimed at modernizing the regulatory framework and enhancing efficiency.

6. CONCLUSION

The proposed risk quantification methodology was developed under the Light Water Reactor Sustainability (LWRS) program, and represents a significant step forward in modernizing the regulatory framework governing nuclear security. By introducing a quantifiable metric for evaluating security risk, the methodology empowers NRC licensees to optimize their physical protection systems while maintaining compliance with regulatory standards. Its optional nature ensures that facilities can choose whether to adopt the methodology based on their operational and financial priorities, providing flexibility and respect for the diverse needs of the commercial nuclear fleet.

For the NRC, the methodology offers a streamlined approach to regulatory oversight, reducing administrative burdens and enhancing consistency across the fleet. It aligns with broader national priorities, supporting energy independence, technological innovation, and economic resilience. By fostering innovation and adaptability in security planning, the methodology ensures that the nuclear industry remains a cornerstone of America's energy strategy.

The pilot study conducted at the Monticello Nuclear Generating Plant demonstrates the feasibility and scalability of the methodology, providing a compelling case for its adoption. Through phased integration and alignment with established industry practices, the methodology can be implemented effectively, ensuring that stakeholders build confidence in its processes and outcomes.

In conclusion, the proposed risk quantification methodology offers transformative benefits for both licensees and the regulator, addressing longstanding challenges while enabling the nuclear industry to adapt to evolving threats and opportunities. Its adoption represents a forward-looking approach to nuclear security, ensuring that the industry remains safe, reliable, and resilient in the face of future challenges. This work satisfies M3LW-25SN1203023 under the LWRS program.

7. REFERENCES

[1] Executive Order 14300 of May 23, 2025, "Ordering the Reform of the Nuclear Regulatory Commission." [Online]. Available: https://www.federalregister.gov/documents/2025/05/29/2025-09798/ordering-the-reform-of-the-nuclear-regulatory-commission

[2] Executive Order 14302 of May 23, 2025, "Reinvigorating the Nuclear Industrial Base." [Online]. Available: https://www.federalregister.gov/documents/2025/05/29/2025-09801/reinvigorating-the-nuclear-industrial-base

[3] Executive Order 14262 of April 8, 2025, "Strengthening the Reliability and Security of the United States Electric Grid." [Online]. Available: https://www.federalregister.gov/documents/2025/04/14/2025-06381/strengthening-the-reliability-and-security-of-the-united-states-electric-grid

[4] Executive Order 14156 of January 20, 2025, "Declaring a National Energy Emergency." [Online]. Available: https://www.federalregister.gov/documents/2025/01/29/2025-02003/declaring-a-national-energy-emergency

[5] S.1111 - ADVANCE Act of 2023, "Accelerating Deployment of Versatile, Advanced Nuclear for Clean Energy Act of 2023," Public Law 118-67, signed into law July 2024. [Online]. Available: https://www.congress.gov/118/plaws/publ67/PLAW-118publ67.pdf

[6] United States Nuclear Regulatory Commission, Title 10, Code of Federal Regulations, § 50.54, "Conditions of licenses," Nov. 16, 2023. [Online]. Available: https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0054.html

[7] United States Nuclear Regulatory Commission, Title 10, Code of Federal Regulations, § 50.90, "Application for amendment of license, construction permit, or early site permit," Aug. 28, 2007. [Online]. Available: https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0090.html

[8] United States Nuclear Regulatory Commission, Title 10, Code of Federal Regulations, § 73, "Physical Protection of Plants and Materials," Mar. 14, 2023. [Online]. Available: https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/full-text.html

[9] National Nuclear Security Administration, "Enterprise Safeguards and Security Planning and Analysis Program," NNSA SD 470.4-2, Jul. 23, 2018. [Online]. Available: https://directives.nnsa.doe.gov/supplemental-directive/sd-0470-0004-2/@@images/file

[10] United States Nuclear Regulatory Commission, "Risk Informed Activities," Jun. 8, 2020. [Online]. Available: https://www.nrc.gov/about-nrc/regulatory/risk-informed/rpp.html

[11] United States Nuclear Regulatory Commission, "Risk and Performance Concepts in the NRC's Approach to Regulation," Jul. 7, 2020. [Online]. Available: https://www.nrc.gov/about-nrc/regulatory/risk-informed/concept.html

[12] United States Nuclear Regulatory Commission, "Staff Requirements - SECY-98-144 - White Paper On Risk-Informed And Performance-Based Regulation," Mar. 1, 1999. [Online]. Available: https://www.nrc.gov/reading-rm/doc-collections/commission/srm/1998/1998-144srm.pdf