DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express 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. Reference 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 United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof. Reference herein to any social initiative (including but not limited to Diversity, Equity, and Inclusion (DEI); Community Benefits Plans (CBP); Justice 40; etc.) is made by the Author independent of any current requirement by the United States Government and does not constitute or imply endorsement, recommendation, or support by the United States Government or any agency thereof.

SAND2025-04485R

Technical Letter Report

TLR–RES/DE/REB–YYYY–NN

Assessment of Physical Security Modeling and Simulation in the Vulnerability Assessment Process

Date: March 2025

Prepared in response to Research Assistance Request NSIR-2024-002, by:

Commie Byrum, Brenton M. Pickrell, Doug Osborn
Sandia National Laboratories

Ellie Cohn, John Matrachisia, Jason Tokey, James Chang, Raj Iyengar
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission

Division of Engineering
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555–0001

DISCLAIMER

This report 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 employee, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product, or process disclosed in this publication, or represents that its use by such third party complies with applicable law.

This report does not contain or imply legally binding requirements. Nor does this report establish or modify any regulatory guidance or positions of the U.S. Nuclear Regulatory Commission and is not binding on the Commission.

ABSTRACT

This report provides a comprehensive assessment of physical security modeling and simulation tools available for use in the vulnerability assessment (VA) process for nuclear facilities. It outlines the historical evolution of VA methodologies, emphasizing the transition from traditional layer-based approaches to a more holistic framework that integrates detection probabilities directly into combat simulations. The document details the critical components of the VA process, including the characterization of targets, threats, and protective measures, as well as the development of adversary scenarios that reflect both insider and outsider threats. It highlights the importance of performance assurance programs, emphasizing the need for continuous evaluation and testing of security systems to ensure their effectiveness against evolving threats. Additionally, the report discusses the significance of utilizing accredited modeling and simulation tools in accredited areas to accurately represent adversary actions and the corresponding responses of protective forces. By establishing a systematic approach to VA, this document aims to enhance the overall security posture of nuclear facilities, ensuring compliance with regulatory standards while effectively mitigating risks associated with potential adversarial actions.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS

AACT	Alarm assessment and communication time
ARAPT	Alarm response and assessment performance tests
ASD	Adversary sequence diagram
ATLAS	Adversary Time-Line Analysis System
ASSESS	Analytical System and Software to Evaluate Safeguards and Security
BATLE	Brief Adversary-Threat Loss-Estimator
C	Consequence value
CC	Correlation coefficient
CDP	Critical detection point
DBT	Design-basis threat
DEPO	Design Evaluation Process Outline
DOE	U.S. Department of Energy
FoF	Force-on-force
FoM	Figure of merit
IDS	Intrusion detection system
LSPT	Limited scope performance test
MC&A	Material control and accounting
Mod/sim	Modeling and simulation
N	Number of iterations
NRC	U.S. Nuclear Regulatory Commission
PA	Protected area
P_A	Probability that an assessor will accurately assess the alarm
P_C	Probability that alarm(s) are properly communicated to the response force
PCC	Partial correlation coefficient
P_E	Probability of system effectiveness
PF	Protective force
P_H/P_K	Probability of hit/kill
P_I	Probability of interruption
PIDS	Perimeter intrusion detection system
P_N	Probability of neutralization
PPS	Physical protection system
P_R	Probability that the responders will maneuver consistent with plans
P_S	Probability that the detection sensor will sense unauthorized activity
P_T	Probability that the sensor will transmit to an assessor
R	Conditional risk
R^2	Square of the regression coefficient
RF	Response force
RFT	Response force time
RIT	Risk-informed timeline
SAFE	Safeguards Automated Facility Evaluation
SBD	Security-by-design

SME	Subject matter expert
SNAP	Safeguards Network Analysis Procedure
SNM	Special nuclear material
SRC	Standardized regression coefficient
SRRC	Standardized rank regression coefficients
UCCATS	Urban Combat Computer Assisted Training System
UQUA	Uncertainty quantification and uncertainty analysis
V&V	Verification and validation
VA	Vulnerability assessment

1 INTRODUCTION

1.1 Purpose and Objective of Research

The purpose of this research is to evaluate the effectiveness of physical security modeling and simulation (mod/sim) tools in the vulnerability assessment (VA) process for nuclear facilities. This report is intended to follow up on ML23346A027, Preliminary Assessment of Physical Protection Modeling and Simulation Tools [1]. This report aims to provide a comprehensive overview of the methodologies, tools, and best practices that can enhance the security posture of these facilities against adversarial threats. By analyzing the historical context and current applications of VA processes, this document seeks to inform stakeholders about the importance of integrating advanced modeling techniques into their security assessments.

1.2 Background

Nuclear facilities are critical infrastructures that require robust security measures to protect against theft, sabotage, and other malevolent acts. The vulnerability assessment process has evolved significantly over time, transitioning from prescriptive security measures to a more risk-informed, performance-based approach. This evolution has been driven by the need to address increasingly sophisticated threats and to ensure that security systems are effective and resilient.

1.2.1 Summary of Current Approaches

Current approaches to vulnerability assessment leverage a variety of mod/sim tools that facilitate the analysis of physical protection systems (PPS). These tools enable analysts to simulate adversary actions, assess the effectiveness of detection and response measures, and identify potential vulnerabilities within the security framework. The integration of performance testing and data-driven methodologies is essential for establishing a comprehensive understanding of the security landscape, allowing for informed decisionmaking regarding resource allocation and system enhancements. This report explores the various components of the VA process, including the characterization of threats and targets, the development of adversary scenarios, and the application of performance assurance programs to ensure ongoing effectiveness of security measures.

2 HISTORY & PURPOSE OF VULNERABILITY ASSESSMENT PROCESS

2.1 History of VA Process

2.1.1 Introduction

This document discusses analysis tools, primarily software tools, for assessing the effectiveness of PPSs at nuclear facilities.

2.1.2 Applications of Vulnerability Assessment Processes to Protecting Nuclear Materials at Nuclear Facilities from Theft and Sabotage.

The operation of a nuclear facility creates risks due to it being a possibly attractive target for malevolent actors, whether the latter are interested in theft of that material, using that material for radiological sabotage of that target, especially if the facility is a nuclear power plant, or other high-consequence objectives. Thus, both the facility and regulatory authorities have a responsibility to assure the public that that risk of such attacks is effectively maintained at an acceptable level.

Historically, the security risk of operating a risk-significant, nuclear facility in the face of the threat of malevolent acts over a period has been conceptually defined as the conditional probability that, given an attack, what is the probability an adversary action will be thwarted in the presence of an adversary attack. This is defined as the probability of effectiveness (P_E), the probability that the PPS will defeat the adversaries before they achieve their objectives,

There are software tools that calculate P_E. These tools can perform hundreds of simulated attacks to provide a realistic estimate of P_E, by a statistical comparison of the number of friendly successes and the number of total iterations. This capability is possible because both friendly and adversary behaviors are modeled in the software and their actions and events also occur within a realistic representation of the site modeled in the software. Each iteration includes probabilities of various decisions by both forces as well as a probability of success for each action intended to neutralize the other party (e.g., shooting a firearm, throwing a grenade, etc.). As a result, no humans have to be “in the loop” to perform each of these simulated attacks; the users set the sequence of runs, the number of iterations (N) and then run the software. After the iterations have been completed, users can interpret the results.

The analyst develops scenarios based on the defined threat characteristics and objectives defined in the DBT and then uses mod/sim to determine P_E for each scenario. . One approach is to have “red teams” of various kinds develop those scenarios. This document does not provide any details about such “red team” approaches since that scenario identification process does not, in general, require use of software.

As discussed in the next Section, P_E can be subdivided into the two components based on the recognition that a PPS can only be effective if interruption occurs (as defined next) AND the adversary is neutralized (also as described below). Based on this model, we write:

Equation 1: Probability of System Effectiveness

$$P_E = P_I * P_N$$

P_I = Probability of Interruption. The probability that the adversary is detected early enough to allow the response force to disrupt adversarial activity before it reaches or achieves its objective.

P_N = Probability of Neutralization. The probability, given interruption of the adversary by the response force, it will gain complete physical control of the adversary force.

The benefit of such models is that they can provide a large amount of data based on many permutations of the same scenario or allow variability in both friendly and adversary force activities to provide areas where the lowest P_I was not a previously identified vector. Combining these equations, one can write R as:

2.1.3 Generic PPS Vulnerability Assessment Process

In the 1970s, a systems engineering framework based on the concept of defining objectives of a system, designing a system to meet those objectives, and then testing the system to determine if it meets its objectives was adopted to physical protection. The process is cyclical, and continued until the final system is determined to sufficiently meet its defined objectives. This process, adapted for conducting VAs for PPSs was defined as the Design and Evaluation Process Outline (DEPO), and is illustrated in Figure 1.

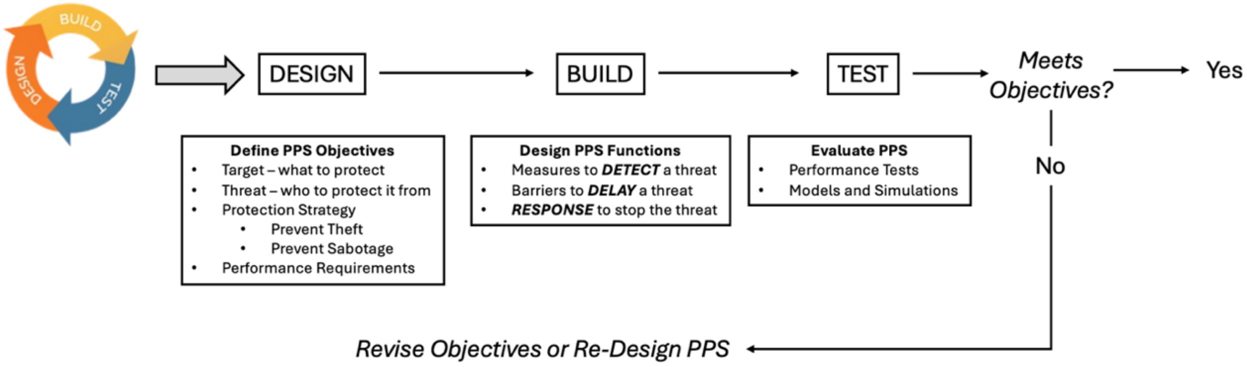


Figure 1 - Design and Evaluation Process Outline (DEPO)

A VA consists of three main phases:

1. Defining PPS Objectives: this phase of a VA involves defining the “target,” or asset being protected, the defined threat the target is being protected against, the protection

strategy, and the performance requirements for meeting the protection strategy against a defined threat.

2. Designing or Characterizing PPS Functions: this phase of a VA involves characterizing the planned or existing elements of a PPS providing the functions of detection, delay, and response.
3. Evaluating the Effectiveness of the PPS: this phase of a VA involves conducting performance tests along with mod/sim as appropriate to estimate the effectiveness of a PPS in meeting its defined objectives.

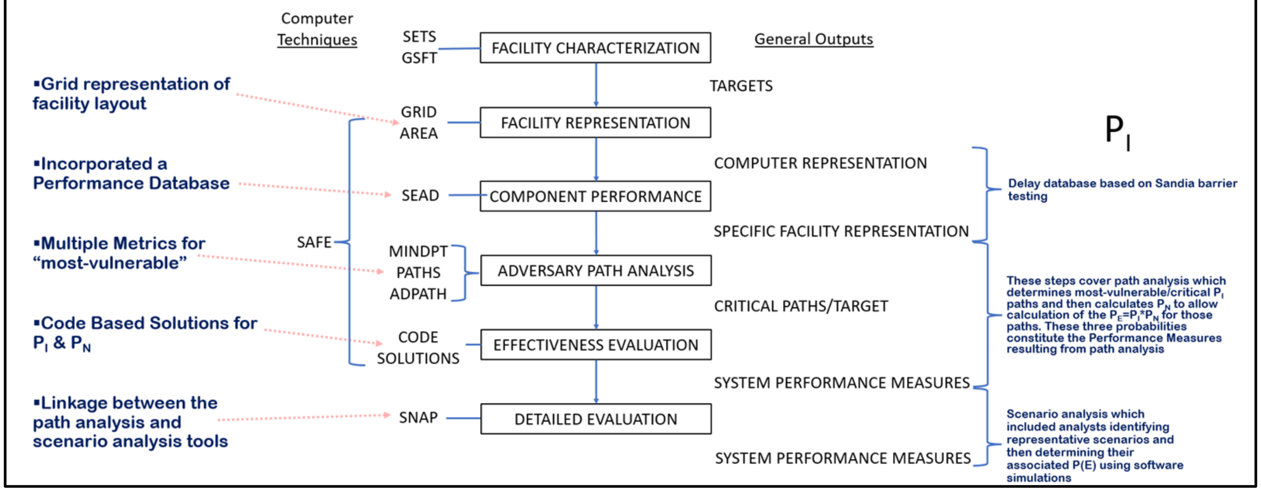
If the evaluation of a PPS determines it meets its objectives, no further action is required. If it is determined that the PPS does not meet its objectives, either the PPS objectives can be re-evaluated and modified as necessary, or the PPS functions can be enhanced until the PPS is determined to meet its objectives.

2.1.4 Development and Application of Mainframe VA Software

The following figure shows the process developed during the 1970s for performing all of those analysis steps listed in the previous figure, along with the names of the corresponding mathematical software tools. Other tools, including the Insider Safeguards Effectiveness Model and the Site Security Evaluation Model are not shown.. The Safeguards Automated Facility Evaluation (SAFE) software was created to perform the vulnerability search using mathematical models, while the Safeguards Network Analysis Procedure (SNAP) software was created to perform constructive simulations to analyze specific scenarios as part of the scenario generation and analysis phase.

Note that the word “Advanced” in this figure is in quotes because the software capabilities listed were advanced for that particular time (an exception being that the facility was described using a grid, rather than just layers of protection as part of Adversary Sequence Diagrams used in later tools).

The SAFE/SNAP Approach had a Number of "Advanced" Features



Computer Techniques

General Outputs

- Grid representation of facility layout
- Incorporated a Performance Database
- Multiple Metrics for "most-vulnerable"
- Code Based Solutions for P_I & P_N
- Linkage between the path analysis and scenario analysis tools

SETS GSFT — FACILITY CHARACTERIZATION

TARGETS

GRID AREA — FACILITY REPRESENTATION

COMPUTER REPRESENTATION

SEAD — COMPONENT PERFORMANCE

SPECIFIC FACILITY REPRESENTATION

SAFE

MINDPT PATHS ADPATH — ADVERSARY PATH ANALYSIS

CRITICAL PATHS/TARGET

CODE SOLUTIONS — EFFECTIVENESS EVALUATION

SYSTEM PERFORMANCE MEASURES

SNAP — DETAILED EVALUATION

SYSTEM PERFORMANCE MEASURES

P_I

Delay database based on Sandia barrier testing

These steps cover path analysis which determines most-vulnerable/critical P_I paths and then calculates P_N to allow calculation of the $P_E=P_I*P_N$ for those paths. These three probabilities constitute the Performance Measures resulting from path analysis

Scenario analysis which included analysts identifying representative scenarios and then determining their associated P(E) using software simulations

Figure 2: The SAFE/SNAP Approach

The modeling details achieved in the SAFE mathematical software tools and in SNAP were useful and positive at the time, but were not as sophisticated as today's simulation tools. The software tools themselves proved to be difficult to access for use by site personnel because they had to be run on mainframe computers at U.S. Department of Energy (DOE) laboratories. Instead, the software was used primarily by security experts working directly with staff at those laboratories.

As indicated by this diagram about SAFE and SNAP, there proved to be great activity and successes from 1975 to 1980 in the development of new computer programs for outsider threat vulnerability analysis. Subsequently, those efforts largely ceased until 1985, when simplified versions of some of these earlier programs were created to run on personal computers and databases of performance values—including probability of detection (P_D) component values—began to appear for use by those programs.

2.1.5 Development and Application of Software to Carry Out Both VA Phases

Between 1984 and 1985, DOE began a process of moving from prescriptive physical security requirements to a risk-based regulatory approach where DOE facility operators had to perform VAs to demonstrate that their PPSs, as documented in master safeguards and security agreements, provided adequately low conditional risk across all threats described in the DBTs. As part of this shift, the DOE funded Sandia National Laboratories and Lawrence Livermore National Laboratory to create a more advanced software package called the Analytical System and Software to Evaluate Safeguards and Security (ASSESS) and to develop courses for site vulnerability analysts. This model incorporated other tools such as the Estimate of Adversary Sequence Interruption code, which analyzed multiple pathways, and the Evaluation of Threats model for evaluating vulnerability to insider threats. From an outsider threat perspective, ASSESS incorporated a module including a path analysis tool to determine the 10 paths through an Adversary Sequence Diagram that had the lowest P_I against several types of adversaries and then incorporated an existing mathematical model, called the Brief Adversary-Threat Loss-Estimator (BATLE), in a separate model for calculating P_N to determine P_E for those most-vulnerable P_I paths. The resulting paths and their associated P_E values were then reviewed and, in some cases, modified to correct for deficiencies in those models. Early versions of ASSESS were released in 1989 and the associated courses were developed to help site analysts use that software. Subsequently various iterations of the software were released that addressed software bugs and provided better functionality in the software.

2.1.6 Development and Application of Man-in-the-Loop Military Simulations for Determining P_N

After several years of using ASSESS, DOE Headquarters and site personnel at most facilities concluded that the ASSESS Neutralization Module, based on the BATLE mathematical model, was too simplistic to accurately model battles between adversaries and defenders. As a separate endeavor, the US Army had been funding Lawrence Livermore National Laboratory to develop weapons effects simulations since the 1960s. Several generations of this software, with different names, were developed for military purposes. Starting approximately in 1992, the following generations of the simulation software began to be used by DOE as more capable tools to model battles between adversaries and response forces:

- Urban Combat Computer Assisted Training System (UCCATS)
- Joint Tactical Simulation
- Joint Conflict and Tactical Simulation

These simulation tools modeled adversaries, protective forces (PFs), and vehicles at an entity-level, allowing human operators operating “in the loop” to control those entities so the latter could carry out detailed attack plans. As a result, these tools could be used, in conjunction with Force-on-Force (FoF) exercises and LSPTs, to determine P_N in much more detail than BATLE allowed for the most-vulnerable P_I paths that came out of ASSESS, once these paths had more details added to them so the resulting scenarios could be performed in these simulations. At the same time, these simulations could be used to determine P_E when P_I was 1, meaning that $P_E = P_N$. Databases for adversary weapons were developed for use in these simulations.

An important limitation of these tools was several humans would have to control these entities and, for the most part, the simulations could not be run much faster than real time. This meant, for example, a 10-minute scenario required at least 10 minutes to run for each replication and often needed more time if a significant engagement between adversaries and response entities required more time to finish. At the time, this was not much of a constraint since the DBTs and response forces at that time could be modeled using a relatively small number of analysts and an administrator which proved to be relatively cost effective compared to FoF exercises.

2.1.7 Next Generation VA Capabilities Adopted in the Early 2000s

In the early 2000s, DOE recognized the need for new VA software tools for the following reasons:

- ASSESS only analyzed delay and did not have the capability to identify key protection elements in the PPS.
- ASSESS required the analyst to jump between five or more separate software modules to perform the necessary VA steps.
- After 9/11, the DBTs changed to the point that running “person-in-the-loop” simulations were impractical for addressing the scenarios and adversary capabilities that needed to be covered.

Note: Key protection elements are defined as protection elements that, if individually degraded to a critical performance level, reduce P_E to an unacceptable value.

To meet the first need, the Adversary Time-Line Analysis System (ATLAS) software program was developed to compute the most-vulnerable paths for outsider adversaries. ATLAS added a new capability not in ASSESS for performing VAs against a violent insider based on P_D values for a non-violent insider that were calculated by the existing ASSESS Insider Module. ATLAS also included all of these capabilities (except for the ASSESS Insider Module models to calculate P_D values) in one software package. Note that there was interest in incorporating the Insider Module P_D generation mathematical models in ATLAS, but the effort was not funded for several reasons including that the second need, for developing or adopting a new constructive simulation for calculating P_N and $P_{E,}$ was deemed by DOE to be much more important to fund.

2.2 Types of Security Mod/Sim Tools

While mod/sim tools range in functionality, in general, they can be grouped into three main categories:

Table 1: Different Types of Mod/Sim Tools

Tool Type	Purpose	Complexity
Path analysis	• Enables simple to complex adversary pathways, critical detection points, and potential vulnerabilities.	Low
Tabletop visualization	• Creates, records, and plays back scenarios developed during tabletop exercises. • Planning tool for performance testing, adversary attack plan modeling, FoF exercises, or other security engagements.	Medium
Combat simulation	• Models complex combat interactions between agents in virtual environments.	High

Note that FoF) exercises and limited scope performance tests (LSPTs) are separate performance tests involving human actors operating directly in an actual, physical environment and for this reason are not discussed here as mod/sim tools. In addition, they are vital for creating plans, validating procedures, verifying results of manual tabletop exercises. FoF exercises and LSPTs provide accurate data and probabilities that should be used in software simulation tools. FoF exercises and LSPTs are often the only way to identify human-related deficiencies such as poor training and competence and individual human factor weaknesses, such as fatigue of both sides during field exercises, all of which are difficult to model in the software simulations and manual tabletop exercises.

A more detailed overview of U.S. Government and commercial mod/sim tools can be found in Appendix B of "*Integration of Safety, Security, and Safeguards During Design and Operations – A Technical Assessment and Regulatory Considerations for Advanced Reactor and Advanced Fuel Fabrication Facilities,"* ML24275A073.

3 MODELING & SIMULATION TOOLS IN VULNERABILITY ASSESSMENT

Mod/sim tools can enhance and expedite VAs for nuclear facilities. These tools provide assessors with deeper insights into the performance of physical protection technologies and response force processes, ultimately improving security measures. To fully leverage the capabilities of these tools, ranging from simple path analysis to complex combat simulations, users should invest in creating accurate models, training personnel, and assembling the right teams to analyze results effectively.

3.1 Importance of Accurate Models

The effectiveness of evaluations conducted using mod/sim tools is directly tied to the accuracy of the facility model. Models should not only represent the physical layout of the facility, including scale and composition, but also realistically portray operational processes, response force actions, verified technological capabilities, barriers and breach times, and DBT capabilities. This comprehensive representation is essential for maintaining the integrity of the evaluation process and ensuring the validity of the results.

3.1.1 Model Development Considerations

3.1.1.1 Modeler and User Capabilities

Utilizing a mod/sim tool should be done by both a modeler, who is responsible for building the digital likeness of a facility within the software with a broad range of software skills and a user who is a security practitioner with a diverse understanding of the facility to be modeled, the scenarios to be represented, and the analyses to be performed. In some cases, the modeler and user is the same person or group of people.

- **Tool skills.** Depending on mod/sim tool selected, the person creating the model for the VA could be a professional model developer or a security specialist from the facility who has been provided user training. If a highly immersive and detailed model is required, 3D model developers can use state-of-the-art modeling software to develop complex digital representations of a facility, which can then be imported into the selected mod/sim tool for analysis. If a simpler model is sufficient for the objectives of the VA, a user with minimal training can use the selected mod/sim tool to develop a simple, but scaled, 3D model that still provides functionality.
- **Analysis proficiency.** Beyond the technical skill of the modeler, the user's input is necessary to ensure accurate placement of PPS technologies and response personnel, and to adequately interpret the results of testing activities.

3.1.1.2 Access to Sensitive Data

To create realistic models, access to sensitive data is critical. This includes:

- **Facility structure and surrounding terrain.**
  - Complete facility blueprints that include location of targets and inherent security system design elements.
  - Structural composition of barriers (e.g., wall rebar, type and configuration, thickness, and psi rating; door materials and thickness(es); etc.).
  - Routine access points, such as doors, windows, hatches, interior and exterior ladders and permanent scaffolding, and person-passable tunnels.
  - Less-noticeable features, such as piping or landscape features that can be climbed.
  - Locations that can be accessed via person-assisted lifts, such as catwalks, mezzanines, or similar locations.
  - Pathways should be identified without regard to time-specific radiological conditions. For example, a pathway that leads into, from, or through a locked high radiation area should be included in a model, because that area may have reduced radiation conditions after reactor shut down, and DBT adversaries are not concerned with health implications that are not immediately incapacitating.
- **PPS technology and personnel performance testing data.** Accurate characterization of a facility model depends on science-based, field-tested data including the following:
  - Component characteristics such as sensor fields, camera functions, breaching time for barriers and technology placement.
  - Response force characteristics such as guard numbers, locations, and response times during all shifts and operational situations (e.g., Limited Scope Performance Tests).
- **Operational procedures and policies.**
  - Locations of operational staff and personnel during all shifts.
  - Policies for personnel movement during emergency situations, such as critical alarms, power outages, acts of sabotage, or natural disasters.
- **DBT documents**
  - Understanding of the types of threats described in the governing DBT(s).

3.1.1.3 Collaboration with Subject Matter Experts (SMEs)

Accurate models benefit from collaboration with SMEs from multiple disciplines, including security personnel (e.g., response team leaders, central alarm station operators, armed responders, etc.), reactor operations staff, plant engineering, radiation protection, site safety specialists, and emergency coordinators. Their insights are vital for understanding the facility's layout, operational complexities, and potential vulnerabilities.

3.1.1.4 Reliable, Validated Inputs

It is critical that all inputs to mod/sim models are tested and valid. Important characteristics to consider when gathering data for a model include:

- **Performance test data.** Physical components should undergo extensive testing under all conditions in which they would be expected to operate. Documentation provided by element manufacturers should be considered as starting points for testing rather than used as the sole source of data to model the equipment. Similarly, materials used for construction should be tested against breaching tools, so accurate data regarding delay elements can be input to the facility model [2].
- **Alternate data sources.** While most mod/sim tools have a publicly available default dataset, for the most accurate analyses, more detailed proprietary datasets should be considered.
    - U.S. Government datasets that are specific to the site, industry, or scenario being tested.
    - Site-specific datasets that result from site-specific testing or operational experience.
    - Performance data from onsite technology and response testing.
- **Past analysis.** Data collected as the result of previous scenario testing or tabletops should be considered. In some cases, datasets already exist for some of the more common aspects of PPSs as they relate to mod/sim.
- **Existing Documents.** When facility models are developed, detailed notes should be kept regarding aspects such as physical testing of security components, materials used in facility construction, and resources and training of site and security personnel. This information can be valuable for those conducting followup analysis and for auditors and inspectors as an additional source of data on testing and the basis for past decisions.

3.1.2 Use of Simplified Models

The complexity and accuracy of a facility model is driven by the types of scenarios or analyses that the user would like to perform. Simplified facility models that are appropriate for one scenario may not be appropriate for a different scenario; for example, a facility model that includes details for a portion of a site—only the exterior areas of an owner-controlled area and protected area (PA)—could not be used to evaluate interdiction and neutralization within other areas of the site (e.g., the interior of a power block).

Models created with simplified physical security elements such as grouped sensors, adversaries, or responders may be inappropriate for some analyses. For example, a facility model that uses a simple line with an overall detection and assessment probability to represent the intrusion detection system (IDS) for a PA isolation zone would not enable a user to identify or evaluate vulnerabilities that may be associated with any specific IDS sensor or assessment component in that zone.

3.1.3 Other Considerations

- **Detailed vs. Screening Tools.** Different mod/sim tools have different uses. Some tools, such as tabletop tools, are not intended to determine the effectiveness of the PPS through results such as P_I or P_E. These tools are instead used to provide the user with more general insights, such as redundancies in action, shortcomings in response or conflicts between responders. For predictive analysis, sites should use pathway analysis (for P_I only) or combat simulation (for P_I, P_N, or P_E) tools.

- **Software and hardware requirements.** Licenses for mod/sim tools for analysis of PPSs vary in both price and availability, as does the hardware required to operate the tools. In addition, some tools are more user-friendly than others, and this affects the degree of effort required to use the tools.

3.2 Advantages of Mod/Sim Tools

Facility operators that use mod/sim tools as part of a VAs should achieve the following benefits:

3.2.1 Resource Management

- **Operational consistency.** Conducting scenarios on a virtual model ensures no interruption to ongoing facility or security operations.

- **Decreased staff interruption.** Conducting live exercises entails extra staff be brought in to conduct the exercise—above staff needed for regular operational needs.

- **Budget Efficiency.** While significant investment is required to stand up a model, once it is established it can be used for an unlimited number of scenarios and testing with little additional cost. Users can perform indepth analyses for very little expense (when compared to the cost of conducting full force-on force (FoF) exercises or constructing or repositioning actual security infrastructure).

3.2.2 Cost-Effectiveness in Assessing PPS

- **Security-by-Design (SBD)**. Mod/sim tools can be used to develop notional facility models that incorporate safety, safeguards, and security principles from the point of inception. With these principles in mind from the outset, users can iteratively design a facility with the desired balance of technologies and response staff that saves money while meeting regulatory requirements.

- **Technology & Procedural Upgrades.** Mod/sim tools can be used to place, move, and/or replace technologies or personnel in a virtual representation of a facility to achieve improved security and cost-effectiveness before any purchases, construction, or staff changes. Mod/sim tools can also provide science-based data to demonstrate adequate protection to regulatory authorities or operational management before implementation of the designed system.

3.2.3 Detailed, Science-based Analyses

- **Probability of Effectiveness.** Mod/sim tools used in a VA assist in determining the probability of effectiveness ($\mathrm{P_E}$) of facility security. This is accomplished by evaluating the probability of interruption ($\mathrm{P_I}$) of an adversary by the response force through a path analysis tool and combining this data with evaluation of the probability of neutralization ($\mathrm{P_N}$) by a response force using a tool to model engagements between an adversary and the facility response force ($\mathrm{P_E = P_I \; x \; P_N}$), or by directly estimating $\mathrm{P_E}$ for a given scenario [3].
- **Unlimited Scenario Exploration.**
    - Mod/sim tools are easily adaptable to any scenario, with reusable and expandable databases.
    - Simulations allow users to explore questions and scenarios without having to experiment on the system itself, enabling the user to play out scenarios that are difficult to replicate in live-action drills, such as explosions, small arms engagements, and radiological or chemical release.
    - Enables users to evaluate their PPSs against the full DBT and beyond DBT scenarios to test the defense-in-depth of a facility.
        - Unconstrained by plant and personnel safety considerations.
        - Unconstrained by exercise artificialities present during FoF exercises, such as timeouts, advance notices (facilitates mental and physical preparation), and limited effects of suppressive fire and precision weapon engagements.
- **Generate detailed records of timelines and events** to support further after-action review, training, and continuous improvement of operational procedures and policies.
    - Running multiple scenarios helps users to identify which variables (e.g., delay, detection, weapons, timelines, etc.) are most important to PPS performance.
    - Mod/sim tools help identify bottlenecks in communication, response timing and procedures.
    - Individual scenarios can be saved and played back at any time to support knowledge transfer and historical records for training as well as regulatory modification testing and evaluation.

3.3 Limitations of Mod/Sim Tools

- **Simplifications and Assumptions.** Depending on the objectives of an evaluation, some assumptions and simplifications regarding facilities can be made in the development of facility models, but great care should be taken to ensure that these simplifications do not impact the integrity of the evaluation. It is also important to note that the more accurately a facility is represented in a model, the better the data resulting from the analysis [4].

- **Challenges in Simulating Human Behavior.** It is challenging to simulate human behavior. Human behaviors in a combat situation are very complicated and cannot always be predicted by simulated representations. These variables should be clearly understood by facility management before interpreting the results of any mod/sim analysis report.
- **Training Requirements.** Some tools require extensive training. Depending on the tools deployed, user training can be both time-consuming and expensive.
- **Not Comprehensive.** Mod/sim tools alone are not a substitute for physical testing of technology elements, FoF exercises or LSPTs. Actual physical tests are irreplaceable with respect to the data provided; they are essential to verifying the output of simulations because they include nearly all the same characteristics of an actual event, where a simulation is limited to representing features and behaviors explicitly modeled.
- **Initial Costs.** There is a large upfront cost to build the facility, defense, and attack scenario models.

4 VALIDATION AND VERIFICATION OF MODELING & SIMULATION TOOLS

4.1 An Introduction of Physical Protection Modeling and Simulation Tool Functions

The applications of physical protection mod/sim tools align with the systems engineering approach laid out in the DEPO methodology which can inform SBD decisionmaking; see Figure 1 for the high-level DEPO flowchart. DEPO is a formal performance-based method that has been used for the design and evaluation of PPS at nuclear facilities for decades [2]. It begins by defining the requirements of the PPS, including the facility and materials to protect; the range of adversaries to protect against; and any policy or regulatory requirements. With consideration of these requirements, a PPS is designed or an existing one characterized in terms of detection, delay, and response. The design is then evaluated using appropriate tools to determine its effectiveness; if ineffective, modification/redesign may be necessary. Any proposed modifications are themselves analyzed in an iterative manner until a design has been found to be sufficiently effective.

The appropriate analytical technique (to include mod/sim tools) used to evaluate the effectiveness of the PPS depends on the needed level of rigor and if quantitative results are necessary or if a qualitative approach would satisfy policy and regulatory requirements. A full-scope VA can be employed when rigorous quantitative results are required [3]. VA is further discussed in Section 5 of this report.

Through the DEPO process mod/sim tools typically include the following functional evaluations:

- **Facility characterization:** This is typically where the first elements of a full-scope model are considered. The facility and building layouts, location of sabotage and theft targets/items, detection, delay, and response elements are typical functional elements included. Initial evaluations of regulatory requirements, such as the DBT, can be included here to ensure the requirements are properly reflected for the further functional evaluations.
- **Pathway analysis:** This is where adversary tactics (e.g., stealth, quickness, or a combination) are evaluated against the detection, delay, and response elements of the PPS design. The only response element considered in pathway analysis is the response force time required to arrive at the point of interruption. It is here where tools can identify the *critical detection point* (CDP), and functional elements such as P_D; see Equation 2. P_D is set for each of the detection elements.
    - **Probability of Interruption:** The resultant adversary pathway timelines can be compared to response force timelines to determine the P_I; see Equation 2. These analyses can be informed through component (detection and delay) performance testing and LSPTs of the response force.
- **Combat simulation:** If not done using results from pathway analysis, combat simulation is where adversary and response force timelines can be integrated to evaluate P_I.

Regardless, combat simulation is used to evaluate P_N. This is done with P_H/P_K (probability to hit/probability of kill) lookup tables.

- **System effectiveness:** This can be included in combat simulations or could be an external calculation to determine P_E; see Equation 3. This metric can be used as the basis for VA results.
- **Security-by-Design:** This can include cost-benefit analysis, justification for security upgrades or strategy changes, and evaluate "what if" scenarios at or above regulatory requirements such as the DBT.

Further discussion of physical protection mod/sim tool function can be found in Reference [2]**Error! Reference source not found.**.

Equation 2: Probability of Detection

$$P_D = P_S * P_T * P_A$$

where:

P_S = The probability that the detection sensor will sense unauthorized activity

P_T = The probability that the sensor will transmit to an assessor

P_A = The probability that an assessor will accurately assess the alarm

Equation 3: Probability of Interruption [5]

$$P_I = P_C * P_D * P_R$$

where:

P_C = The probability alarm notifications are sent & cognized by responders in suitable time

P_R = The probability that the responders will prepare and maneuver consistent with the physical protection program

Equation 1: Probability of System Effectiveness; see above in paragraph 2.1.2

$$P_E = P_I * P_N$$

4.1.1 Risks of Using Inaccurate Data or Tools for Unaccredited Functions

It is important to understand that using notional or anecdotal data and likely most open-source data could lead to inadequate PPS modeling that, in turn, would identify unrealistic vulnerabilities. If blindly implementing the results obtained from the model, it may lead to improper allocation of valuable security resources. NRC has datasets which can be provided to licensees upon request and work with other U.S. Government agencies to identify additional datasets which upon review and approval by NRC could be applicable for licensee needs.

Additionally, certain physical protection mod/sim tools are accredited for only certain functions. For example, the Dante computer code is partially accredited for neutralization analysis. It is important to not only work with the originator of the tool (vendor or U.S. Government agency) but also NRC when it comes to ensuring accreditation for functional evaluations. As mod/sim tools are updated, application accreditations can change; it may be that Version 1.0 of a tool is not accredited for pathway analysis while Version 2.0 is. Such updates should be discussed with NRC to further understand if a version change further accredits a tool for added functional evaluations.

4.2 Software Validation and Verification

Verification & Validation (V&V) is a process to determine the appropriateness of software tools as part of the accreditation process.

Verification is “The process of determining that a model, simulation, or distributed simulation, and associated data accurately represent the developer’s conceptual description and specifications.”

Validation is “the process of determining the degree to which a model, simulation, or distributed simulation, and associated data are an accurate representation of the real world from the perspective of the specific intended use. Validation across the mod/sim life cycle entails application of relevant referent data to refine mod/sim accuracy.”

The important factor is for the user to know which function(s) a particular mod/sim tool is accredited to perform and to what extent. Maintaining a copy of the V&V report for each tool used is recommended.

4.3 Best Practices for Security Modeling and Simulation

Best practices for security mod/sim in VAs include: scenario baseline analysis, comparisons of mod/sim results with real-world conditions, and evaluations of FoF exercises. Scenario baseline analysis involves creating a set of representative scenarios that reflect various potential threats and operational conditions. These scenarios serve as benchmarks for assessing the effectiveness of security measures. Comparison of mod/sim with real-world conditions focuses on validating the accuracy of modeling results by comparing them with actual performance data from security operations. This helps identify discrepancies and refine models. Evaluations of FoF exercises offer insights into the practical effectiveness of security measures by simulating real-world engagements using human participants in the subject environment. Data from these exercises can inform future assessments and improve overall security strategies. Finally, methods for assessing the impacts of variable manipulation on modeling outcomes such as sensitivity analysis, uncertainty quantification, and uncertainty analysis vastly enhance the reliability of the VA process.

Sensitivity and uncertainty analysis methods may be considered to provide greater insight in the validity of the results, and an understanding of critical elements of a PPS that could result in different results if the assumptions and data of their performance is not accurate. The following sections are approaches that are used in the conduct of safety and hazards assessment analyses and might be considered when relying on the use of models and simulations to estimate the effectiveness of a PPS.

4.3.1 Sensitivity Analysis

There are several approaches to sensitivity analysis that can be used in conjunction with a sampling-based uncertainty analysis. Some of these sensitivity analysis approaches are listed and briefly summarized below. In this summary:

- x_j is an element of a vector **x** = $[\mathrm{x}_1,\mathrm{x}_2,\ldots,\mathrm{x}_{\mathrm{nX}}]$ of epistemically uncertain analysis inputs.
- y_k is an element of **y**(**x**) = $[\mathrm{y}^1(\mathbf{x}), \mathrm{y}^2(\mathbf{x}), \ldots, \mathrm{y}^{\mathrm{nY}}(\mathbf{x})]$.
- $\mathbf{x}_i$ = $[\mathrm{x}_{\mathrm{i}1}, \mathrm{x}_{\mathrm{i}2}, \ldots, \mathrm{x}_{\mathrm{i,nX}}]$

  Where *i* = $1, 2, \ldots, \mathrm{nS}$, and is a random or Latin hypercube sample from the possible values for **x** generated in consistency with the joint distribution assigned to the x_j,

- $\mathbf{y}_i$ = $\mathbf{y}(\mathbf{x}_i)$ for *i* = $1, 2, \ldots, \mathrm{nS}$, and (v) x_{ij} and y_{ik} are elements of $\mathbf{x}_i$ and $\mathbf{y}_i$, respectively.

Correlation. A correlation coefficient (CC) provides a measure of the strength of the relationship between x_j and y_k. A linear CC is a common special case of a CC, but any function can be used for a CC. The linear CC between x_j and y_k is equal to the standardized regression coefficient (SRC) in a linear regression relating y_k to x_j and is also equal in absolute value to the square root of the R^2 value associated with the indicated regression. When calculated with raw (i.e., untransformed) data, the CC is often referred to as the Pearson CC. Additional information can be found in References [6, 7].

Regression Analysis. Regression analysis provides an algebraic representation of the relationships between y_k and one or more x_j's. Regression analysis is usually performed in a stepwise fashion, with initial inclusion of most important x_j, then two most important x_j's, and so on until no more x_j's that significantly affect y_k can be identified. Variable importance is indicated by order of selection in the stepwise process, changes in the square of the regression coefficient (R^2) values as additional variables are added to the regression model, and SRCs for the x_j's in the final regression model; see Table 2. A display of regression results in the form shown in Table 2 is very unwieldy when results at a sequence of times are under consideration. In this situation, a more compact display of regression results is provided by plotting time-dependent SRCs. Additional information can be found in References [6, 7].

Table 2: Example of Stepwise Regression Analysis to Identify Uncertain Variables Affecting PE for a Notional Facility

Step[a]	Variable[b]	SRC[c]	R^{2}[d]
1	*Responder P_H/P_K*	0.718	0.508
2	*P_D in isolation zone*	0.466	0.732
3	*Time to breach reactor building*	0.246	0.792
4	*P_D in turbine building*	0.129	0.809
5	*Responder movement speed*	0.070	0.814
6	*Illumination from sunlight*	0.063	0.818

[a] Steps in stepwise regression analysis.
[b] Variables listed in the order of selection in regression analysis.
[c] SRCs for variables in final regression model.
[d] Cumulative R^2 value with entry of each variable into regression model.

Partial Correlation. A partial correlation coefficient (PCC) provides a measure of the strength of the relationship between y_k and x_j after the effects of all other elements of **x** have been removed. For example, a PCC measuring the relationship between P_E and the removal of each of the responder positions could be used to identify the most effective response force posts. Similarly to SRCs, PCCs can be determined as a function of time for time-dependent analysis results. Additional information can be found in References [6, 7].

Rank Transformations. A rank transformation replaces values for y_k and x_j with their corresponding ranks. Specifically, the smallest value for a variable is assigned a rank of 1; next largest value is assigned a rank of 2; tied values are assigned their average rank; and so on up to the largest value, which is assigned a rank of *nS*. Use of the rank transformation converts a nonlinear but monotonic relationship between y_k and x_j to a linear relationship and produces rank (i.e., Spearman) correlations, rank regressions, standardized rank regression coefficients (SRRCs) and partial rank correlation coefficients. In the presence of nonlinear but monotonic relationships between the x_j and y_k, the use of the rank transform can substantially improve the resolution of sensitivity analysis results; see Table 3. Additional information can be found in References [6, 7, 8].

Table 3: Comparison of Stepwise Regression Analyses with Raw and Rank-Transformed Data for PE of a Notional Facility

	Raw Data			Rank-Transformed Data		
Step[a]	Variable[b]	SRC[c]	R^2[d]	Variable[b]	SRRC[e]	R^2[d]
1	*Responder P_H/P_K*	0.562	0.320	*Adversary explosives mass*	–0.656	0.425
2	*Adversary explosives mass*	–0.309	0.423	*Responder P_H/P_K*	0.593	0.766
3	*Adversary movement speed*	–0.164	0.449	*Time of day*	–0.155	0.802
4	*Adversary weight limit*	–0.145	0.471	*Adversary movement speed*	–0.152	0.824
5	*Alarm assessment time*	–0.120	0.486	*Responder movement speed*	0.143	0.845
6	*Time of day*	–0.101	0.496	*Number of offsite responders*	0.120	0.860
7				*Adversary weight limit*	–0.010	0.869

[a] Steps in stepwise regression analysis.
[b] Variables listed in order of selection in regression analysis.
[c] SRCs for variables in final regression model.
[d] Cumulative R^2 value with entry of each variable into regression model.
[e] SRRCs for variables in final regression model.

4.3.2 Uncertainty Quantification and Uncertainty Analysis

Typically, the goals of uncertainty quantification and uncertainty analysis (UQUA) are to confirm the robustness of results from a mod/sim analysis, identify the most likely outcomes, and develop insights into the overall sensitivity of results to key uncertain inputs. The set of uncertain input parameters should yield mod/sim results in which the evaluation of the feasibility of the additional studies for more focused efforts is considered (e.g., additional performance tests for specific security elements or technologies to reduce overall uncertainty within the PPS). In the design and implementation of analyses for complex systems, it is useful for UQUA to distinguish between two types of uncertainty: aleatory uncertainty and epistemic uncertainty [9, 10, 11, 12, 13, 14, 15, 16, 17, 18].

Aleatory uncertainty arises from an inherent randomness in the properties or behavior of the system under study. For example, the weather conditions at the time of an attack are inherently random with respect to our ability to predict the future. Other potential examples include the variability in the properties of a population of detection components experiencing false alarms or nuisance alarms and the variability in the possible future environmental conditions that a PPS component could possibly be exposed to.

Epistemic uncertainty[*] derives from a lack of knowledge about the appropriate value to use for a quantity that is assumed to have a fixed value in the context of a particular analysis. For example, the physics of a detection sensor limit at which a given adversary action would alarm for a specified set of conditions is fixed but not amenable to being unambiguously defined. Other possible examples include minimum voltage required for the operation of a system and the maximum temperature that a system can withstand before failing.

The analysis of a complex system typically involves answering the following three questions about the system:

- What can happen? (Q1)
- How likely is it to happen? (Q2)
- What are the consequences if it happens? (Q3)

And one additional question about the analysis itself:

- How much confidence exists in the answers to the first three questions? (Q4)

The answers to questions (Q1) through (Q3) can require the characterization of epistemic or aleatory uncertainty, depending on which aspect of a given question is being considered. For example, answering (Q2) about a microwave sensor alarming on the passage of a bird has aleatory aspects (e.g., the likelihood of a bird taking a specific path through the detection field) and epistemic aspects (e.g., the likelihood of the sensor entering an alarm state due to the signal generated by a specific alarm pathway.). Posing and answering questions (Q1) through (Q3) gives rise to what is often referred to as the Kaplan/Garrick ordered triple representation for risk [19]. And while the Kaplan/Garrick triple representation for risk does well for safety evaluations, it is important to note that when translated to threat, vulnerability, and consequence, it does not mathematically hold for security risk; this is discussed further in Section **Error! Reference source not found.Error! Reference source not found.**.

In contrast to questions (Q1) through (Q3), (Q4) is a question about the quality of answers to the preceding questions. Uncertainties exist in the answers to the Kaplan/Garrick triple representation for risk, and the process of UQUA is used to determine the degree to which uncertainties affect the answers. Commonly, this is used to establish a level of confidence in different values of an answer. For a given scenario, the true value of P_E is unknown. However, based on performance testing and modeling, probabilities can be calculated that the true value of P_E is greater than or equal to some value (e.g., using notional data, there is a 50 % probability that the true value of P_E is 0.89 or greater and a 95 % probability that the true value of P_E is 0.75 or greater). This is referred to as the "confidence level" or "confidence" in a value.

Existing datasets or well documented site-specific data can be used for UQUA and, depending on the amount and quality of the data, either frequentist or Bayesian statistics can be applied to

[*] Strictly speaking, some parameters may have both aleatory and epistemic attributes but can be treated as epistemic for analytic convenience.

create uncertainty distributions. However, there are likely elements or technologies within the PPS that lack the necessary data to create uncertainty distributions. In these cases, a formal expert judgment elicitation process should be used [20, 21, 22, 23, 24, 25, 26, 27, 28, 29]. In general, a formal expert judgment elicitation process involves a large number of topical area experts to provide a robust uncertainty distribution estimate [30, 31]. However, the resources and schedule typically constrain such an effort and a reduced set of uncertainty distribution elicitations are made on input parameters which are viewed to yield the greatest changes to output metrics of interest. Yet, whenever possible, UQUA should detail a technical basis for parameters to include as uncertain inputs and their distributions.

The use of uncertainty distribution tools such as the risk-informed timeline (RIT) tool allows for the integration of both performance data and expert judgment [32, 33]. The RIT tool leverages Monte Carlo analysis to evaluate adversary and response force timelines utilized in PPS evaluations. This method then utilizes Bayesian updating to combine expert elicitation and small performance test datasets in a consistent and defensible way. The RIT tool allows for a more holistic view of delay performance by providing distributions of task times and task success probabilities to account for adversary tasks that, if failed, would result in failure of the attack. Figure 3 provides a notional example of results from performing a Monte Carlo analysis on a delay task time distribution which combines both limited performance data and expert elicitation.

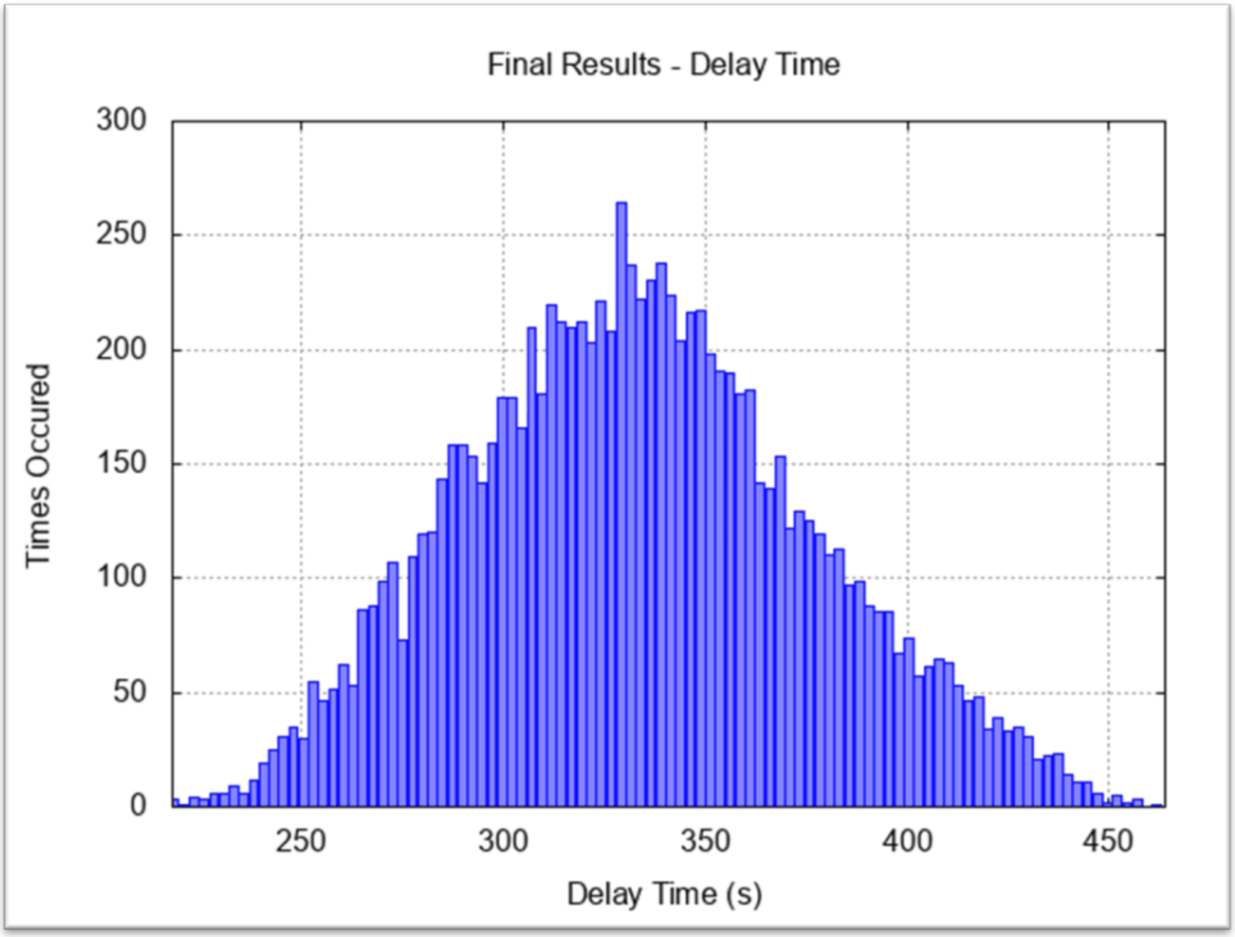


Figure 3: Example of a delay histogram generated by the RIT tool with 10,000 runs. Note that no data here is representative of actual test data

5 OVERVIEW OF THE VULNERABILITY ASSESSMENT PROCESS

5.1 Conducting Vulnerability Assessments

VAs may be conducted for a variety of reasons, including the following:

- Determining the P_E of a site/facility's PPS.
- Evaluating the effectiveness of a new PPS design before its construction.
- Responding to proposed changes in mission or operations.
- Providing a technical basis for changes to a protection strategy.
- Responding to changes in the NRC DBTs.

If sites choose to use a VA, then sites should follow the processes outlined in this Section when conducting VAs. Additionally, sites should consider the following guidelines:

- Scenarios used in a VA should be characterized based on the DBT.
- At a minimum, NRC-licensed sites should review VAs triennially to incorporate applicable performance testing data.

5.2 Process

Conducting a VA involves completing the three phases described in Section 2.1.3:

1. Defining the Objectives of a PPS
2. Characterizing the PPS
3. Evaluating the PPS

Figure 3 outlines the three phases of a VA. Each block in the process flow diagram corresponds to a subsequent section where it is described in greater detail. The characterization processes in a VA may not always follow linear sequence, and in some cases may be completed simultaneously. Other process steps rely on preceding steps.

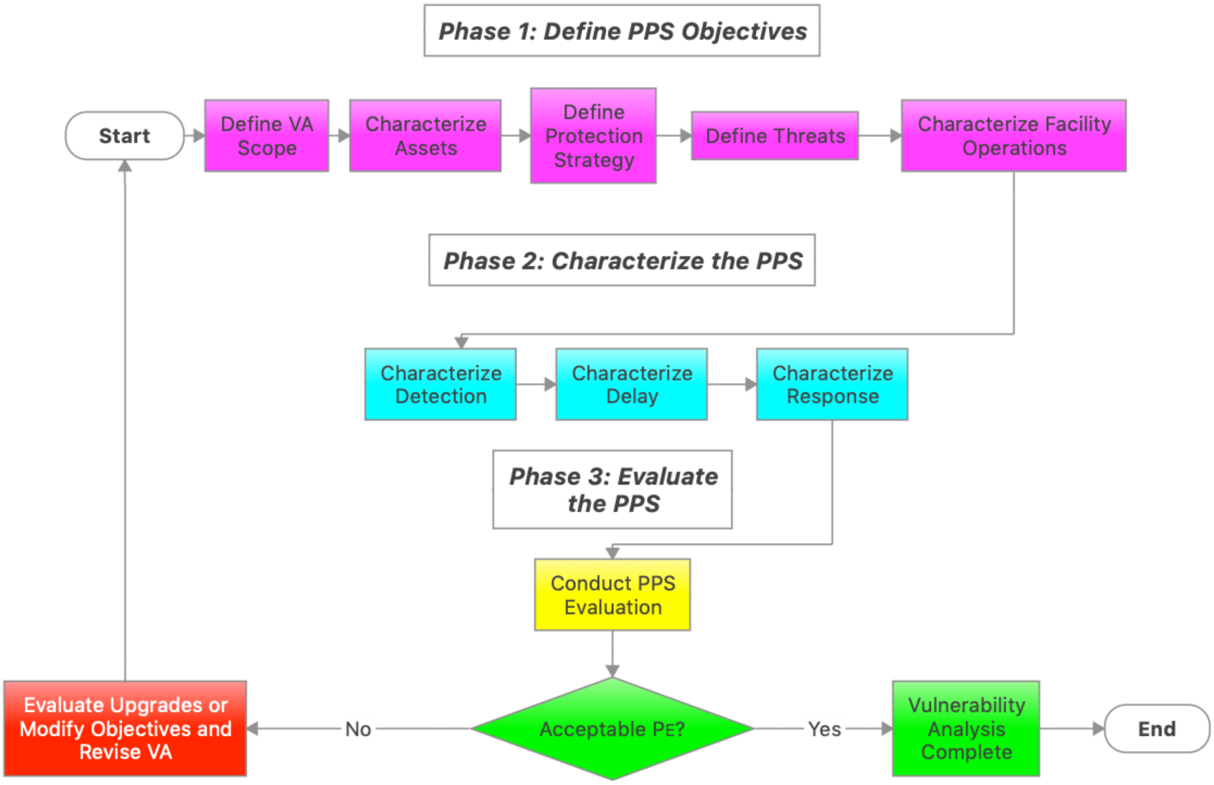

Phase 1: Define PPS Objectives
Start
Define VA Scope
Characterize Assets
Define Protection Strategy
Define Threats
Characterize Facility Operations
Phase 2: Characterize the PPS
Characterize Detection
Characterize Delay
Characterize Response
Phase 3: Evaluate the PPS
Conduct PPS Evaluation
Acceptable PE?
No
Yes
Evaluate Upgrades or Modify Objectives and Revise VA
Vulnerability Analysis Complete
End

Figure 4: Outline of the Vulnerability Assessment Process

5.3 Phase 1: Define PPS Objectives

5.3.1 !Unexpected End of Formula**Define VA Scope**

The first step in a VA consists of defining the objectives of a PPS. This involves defining the scope of a VA—basic requirements, expectations, and assumptions for conducting the VA. This is an essential first step in this process.

The scoping agreement outlines the reason for the conduct of the VA, threat definition, applicable targets, analysis process, key assumptions, schedule, and requirements for the VA. Rather than providing results, it establishes the methods and timeline to obtain them. As the VA evolves, the agreement should be updated to reflect changes. The analyst should fully understand why the analysis is being conducted before conducting the analysis.

VA scoping agreements for NRC-licensed sites should include the following content:

- **Reason(s) for conducting the VA.** Describe the reason or reasons for conducting the VA. What specific driver requires a new analysis of the site security? Driver examples include: the construction of a new facility, a new target location, a different response force configuration, inclusion of performance testing data, or a new threat policy. The explanation should include both background and current information.

- **Changes since the last VA.** Describe what has changed since the last security analysis, including any interim security measures that have not been incorporated into the security analysis. The intent is to be able to trace the evolution of site security postures back to specific requirements and changes in the threat environment.
- **Site-specific assumptions and basis.** Report the following conditions and performance assumptions in the scoping agreement:
  - Target and threat bounding conditions. Describe the adversaries and objectives included in the analysis and how the site is bounding targets for the VA. Provide rationale for why it is appropriate to bound targets into a baseline set or exclude adversary objectives from the analysis.

  - Performance assumptions. Performance assumptions are documented in cases where there is no testing data to support a Figure of Merit (FoM) that will be used in the analysis. For sensing, assessment, and delay FoMs, describe the expected assumptions by system, FoM, and the rationale for use. Assumptions in the scoping agreement are stated by referencing the source of the data to provide NRC with an indication that not all data is supported by performance testing. The following statement provides an example of a detection assumption at the PA layer:

    Detection FoMs for alarm systems contained within the PA can be derived from generic data derived from the Hypothetical Facility Data Handbook (HFDH) [34].

    It is recognized that an assumption that was not previously identified may arise during the analysis. In these situations, the scoping agreement should be updated. The following are example tables using notional data.

Table 4: Example of Figures of Merit Sensing Assumptions

ELEMENT	LAYER	FoM*	FoM DERIVED FROM	ADDITIONAL NOTES
Picture Badge	PA	0.40	Performance Testing	Testing conducted over a two-month period. See Site XX Access Control Performance Test Report PT-1234.
Microwave	PA	0.70	HFDH	
***No data here is representative of actual test data**				

Table 5: Example of Figures of Merit Assessment Assumptions

ELEMENT	LAYER	FoM*	FoM DERIVED FROM	FoM DESCRIPTION
Closed-Circuit Television Camera	PA	0.95	SME	
General Observation	PA	0.02	HFDH	
***No data here is representative of actual test data**				

Table 6: Example of Figures of Merit Delay Time Assumptions

ELEMENT	DESC	LAYER	FoM*	DEFEAT METHOD	FoM DERIVED FROM	FoM DESCRIPTION
Fence	2.4 m chain link mesh fence	OCA	10 s	Handtools	HFDH	
Exterior Wall	20 cm reinforced concrete wall	Vital Area	120 s	Explosive	HFDH	
***No data here is representative of actual test data**						

- **Deviations from NRC requirements.** Describe all current approved exemptions from NRC requirements and uses of alternative measures that are expected to affect the security analysis, including the specific requirement(s) that are being exempted and how alternative security measures or site-specific (e.g., topology, adjacent water sources, nearby facilities/items that may be acted upon to produce a diversion) considerations are expected to affect the VA process.

- **Schedule for conducting the analysis and producing the VA report.** May also include the periodicity of status reporting requirements.

- **Change control process for updating the scoping agreement**. Describe the process and notification chain for information references used for site-specific performance data and provide a table of references to be used to develop site-specific performance data. The table should include the reference, the date of publication of the reference, and a brief description of what performance data is derived from the source. The following is an example of one possible entry into such a table.

Table 7: Example of Sample Information Reference Table

REFERENCE	PUBLICATION DATE	DERIVED PERFORMANCE
HFDH	2021	• Sensor performance metrics

		• Barrier delay metrics • Barrier defeat methods

5.3.2 Target Characterization

Detailed knowledge of a facility’s structures, systems, and components (SSCs) is required to understand the ways adversaries, both insiders and outsiders, might attempt to attack targets. To validate target assumptions, it is necessary to spend time in the facility and vital areas/material access areas, as appropriate, at a site. VA analysts are expected to observe activities at or near a target to validate target assumptions used in VA analysis.

5.3.3 Target Determination

The following process is used for target determination and identifying and characterizing targets at a site.

1. **Identify Potential Target(s).** In determining potential targets, all identified vital areas/material access areas and SSCs need to be evaluated for inclusion in the target set.

2. **Characterize Target(s).** This questions listed for step apply to Category I special nuclear material (SNM) facilities only. See the definitions in 10 CFR 73.2 for the characterization of different types of SNM. Identify basic attributes of each SNM target in order to support target screening and the target bounding processes. Any characterization of target sets, in consideration of sabotage threats, would be done using different questions not discussed in this paper.

    a. Material Configuration

    i. Where is the material located?

    ii. Is the material accessible?

    1. If so, how long does it take to access?

    iii. Is the material moved?

    1. If so, to where and how often?
    2. How long is the material in its different locations?

    iv. Is the material generally kept in a container or other protective enclosure?

    1. If so, is it removed from its primary container or other protective enclosure?

v. Is the material removed for shipments and receipts?

1. If so, where is the SNM stored for shipments and receipts?

2. How often do these movements occur?

b. Target Configuration. The set of target configurations determine the number of different operating configurations required in computer facility models used for pathway analysis and combat simulation. The analyst should collect all the relevant information about containers, enclosures, and other information regarding the way the target material is stored.

i. What are the container's dimensions, shapes, and weights?

ii. What are the task times when material is moved or removed from its container?

iii. Does the adversary need to remove the material from the container in order to accomplish their objective?

iv. Are specialized tools or equipment used to remove the material from its container?

1. If so, how and where are they stored and controlled?

2. What are the task times to remove the material without these tools?

v. Are labels and tamper indicating devices present?

vi. What internal and external shielding do the target and its container have?

c. Target Attributes. The analyst should collect the following information about the specific target material.

i. Material type

ii. Dimensions and shapes

iii. Portability

iv. Dose rate or other self-protection information

v. Material form, e.g., is the material metallic?

3. Screen Targets.

a. Targets can be removed from analysis if the targets have a dedicated barrier or inherent design that exceeds the adversary capabilities in the NRC DBT to complete a malevolent act.

b. Document any target removed from analysis and the rationale for removal.

4. Bound Targets.

   a. To assist in managing the scope of the required analysis, targets may be bound (i.e., assumed to have the same results) using the following parameters:

      i. Protection Measures. Targets that have the same types of detection, delay, and response systems can be bound together.

      ii. Adversary Objective. Targets with the same adversary objectives may be bound together (e.g., theft of SNM or sabotage of vital equipment) if the criteria outlined is met.

      iii. Targets undergoing dissimilar operations cannot be bound together.

5.3.4 Define Protection Strategy

In this step of the VA, the protection strategy of the PPS is defined. For a PPS designed to protect against theft, the objective is to prevent adversaries from leaving a site with material. For a PPS designed to protect against sabotage, the objective is to be able to prevent adversaries from either accessing locations within the site that contain all elements of a target set or completing sabotage acts on all elements of a target set.

5.3.5 Define Threats

Potential threats are defined as two types, outsiders and insiders. Outsider threats are people who do not have authorized physical or logical access to a site or a site's computer assets. Insider threats are people who have authorized physical or logical access to a site or a site's computer assets.

For NRC reactor facilities, the general threat information required to develop applicable threat characterization is found in Regulatory Guide (RG) 5.69, *"Guidance for the Application of the Radiological Sabotage Design-Basis Threat in the Design, Development, and Implementation of a Physical Security Program that meets Title 10 of the Code of Federal Regulations Section 73.55 Requirements."* All applicable NRC memoranda should be reviewed for additional threat clarifications and guidance.

For NRC Category I facilities where radiological sabotage may occur, threat information can be found in RG 5.70, "*Guidance for the Application of the Theft and Diversion Design-Basis Threat for Category I Fuel Cycle Facilities*." All applicable NRC memoranda should be reviewed for additional threat clarifications and guidance.

A threat characterization results in a detailed description of the threat by an adversary to the site's PPS and targets. The description usually includes information about the potential actions, motivations, physical capabilities, and site-specific tactical considerations of potential adversaries.

1. Identify Adversary Types.
2. Identify Adversary Numbers.
3. Establish Adversary Objectives.

All adversary capabilities are considered up to and including the maximum set of capabilities described in the DBT(s). However, not all capabilities may be necessary for all scenarios.

5.3.5.1 Generating a Target Matrix

A site target matrix can developed describing targets to analyze along with their associated threat protection strategy. A target matrix describes the site's targets, and which targets have been bound together. This listing forms the basis for security analysis and planning. **Error! Reference source not found.** is an example of a site target matrix using notional data.

Table 8: Example of Site Target Matrix

AREA	LOCATION	ASSET CATEGORY	TARGETS	THREAT	THREAT TYPE	OBJECTIVE	PROTECTION STRATEGY	BOUND TARGET
PA	Power Block Main Control Room	Vital Area	Controls	Maintenance Worker	Insider	Sabotage	Denial	N/A
	Spent Fuel Pool	Vital Area	Spent Fuel Pool	Terrorist	Outsider	Sabotage	Denial	N/A
	CAS/SAS	Vital Area	Equipment/ Personnel	Terrorist	Outsider	Sabotage	Denial	N/A
	Vault I	SNM	Category I Material	Terrorist	Outsider	Theft	Containment	N/A

5.3.6 Facility Characterization

Characterizing a facility/site is critical to conducting a VA. Every aspect of the facility is examined to accurately model the facility and its operations. Much of the facility information can be obtained through reviews of documentation. However, as-implemented information on facility operations remains best captured from spending a significant time in the field observing activities.

The VA analyst should be fully versed in the following information:

1. **Target.** The VA analyst should be aware of all targets and their locations for all states and conditions the facility operates under.

2. **Facility States.** The VA analyst should understand all facility states—e.g., operational, non-operational, maintenance, refueling, dayshift, backshift, emergency conditions, and other site-specific/facility-specific conditions.
3. **Facility Operations.** To characterize the facility, the VA analyst should thoroughly understand all security-related facility operations. Care should be taken to ensure that the characterization is accurate to the current operations employed by the facility. As

facility operations may change over time, the VA analyst should be alerted to all modifications to the facility since the previous characterization. The VA analyst should also consider whether each operation is a temporary or long-term activity. Facility operations to consider include, but are not limited to:

a) **Facility Operating States.** The analyst should understand all the operational states and conditions under which the facility functions. All facility states should be considered and documented during facility characterization.

b) **As-Built Accuracy.** The facility is modeled (characterized) as it was built, accurately reflecting barriers, sensing, assessment, and delay systems.

c) **FoM. A** FoM is a value used to represent a characteristic of the protection system regardless of the analytical tool/methodology being used to calculate the P_E. FoMs used for P_I include detection, delay times, and response force time. To the extent possible, an FoM should be based on performance testing (e.g., LSPTs) This means an FoM in mod/sim tools should reflect actual performance, and not an upper or lower threshold or an expected performance value.

5.4 Phase 2: Characterize the PPS

5.4.1 Characterizing Detection

Detection is the discovery of potential adversary action attempting to complete a malevolent act. The detection functions include intrusion detection and entry control. Intrusion detection systems are designed to detect unauthorized intrusion to an area being protected, and entry control systems are designed to ensure only authorized personnel are allowed entry or exit to an area, to detect unauthorized entry or exit attempts, and to detect people attempting to bring unauthorized material into an area or to detect people attempting to remove protected assets, such as SNM, from an area without authorization. Detection can be accomplished by the use of technical systems or by people.

Characterizing detection involves developing FoMs for detection of various adversary acts, such as crossing a PA perimeter on foot equipped with an intrusion detection system and video assessment cameras, attempting to enter through an access control point with a falsified credential, etc. Note that FoMs for detection are dependent on the methods and tactics used by adversaries. For example, an adversary could attempt to enter a PA through an access control point using force, stealth, or deceit. An example of force would be for an armed adversary to enter an access control point, engage the guards with weapons fire, and enter the area. An example of stealth would be for an adversary to hide in a compartment in a vehicle entering the area in attempt to enter undetected. An example of deceit would be for an adversary to create a fake credential or steal an authorized credential and attempt to use it to enter the area. Each of these would have a different detection probability.

5.4.2 Characterizing Assessment

Assessment is the capability to determine if the cause of an alarm and if it is caused by adversary intrusion. Characterizing assessment involved developing FoMs following the initial sensing of an adversary act. These FoMs depend on the adversary tactics being used and the method of detection that occurred.

5.4.3 Characterizing Interdiction

Interdiction is the capability for response to arrive in a location in a fashion that causes adversaries to stop their attack actions. This capability depends on the adversary delay time and the response time.

Delay time is that an adversary requires to complete an action or to traverse an area. Analysts should understand the source of delay data and understand the range of delay times associated with a specific task. Note that the delay time to perform a task (e.g., defeat a specific barrier) depends on the method used by adversaries, rather than being an inherent characteristic of the task. At a minimum, analysts should be able to describe the minimum and median times for a given task and understand how this affects delay. Furthermore, as a facility's protection system performs no actions until after the detection of adversaries, delay before detection does not contribute to the overall effectiveness of the protective system. Travel distances are computed as time and treated as delay.

Breaching physical barriers takes time, which is imposed on adversaries as delay. The breaching method used determines the delay the barrier provides. Explosive breaching of barriers may provide additional detection caused by the sound of the breach. Breaching times for a given barrier and defeat method are best understood as a distribution, incorporating uncertainties associated with breaching tasks. In cases where the available performance data is limited, all useful testing results should be included rather than only using one data point (e.g., upper bound, lower bound, most recent test results, etc.) Breaching times are important to the model, and the source and treatment of delay times used should be documented. For example, depending on the model or simulation used, delay times for breaching a wall with explosives might be expressed as single point values or as a positive sinusoidal distribution that can be placed in the modeling/simulation tool as data.

5.4.4 Characterizing Response

The objective of the response characterization is to accurately characterize the response capability against a defined threat to neutralization in the context of the NRC DBT and an identified target. Response characterization is dependent on the analyst observing the response in operation during all conditions and states. To ensure that the VA analyst is evaluating and characterizing response operations based on up-to-date information, field visits and evaluations are conducted, and the results are used in determining P_N.

As part of the response characterization step, the VA analyst should obtain site-specific response information (discussed in the following subsections) to serve as a foundation to characterizing the response.

5.4.4.1 Response Staffing Levels and Locations

The VA analyst should obtain all response staffing levels and positions for all conditions and states and response plans for the building(s) containing targets to be analyzed. A target building may have response staffing levels or assigned locations that are changed with different operating modes. In this case, the response levels and locations should be characterized separately for different modes. Some examples of different operating modes can include the following:

Table 9: Examples of Response Conditions and States

Boiling-water reactor	Pressurized-water reactor
Mode 1: Power Operation	Mode 1: Power Operation
Mode 2: Startup	Mode 2: Startup
Mode 3: Hot Shutdown	Mode 3: Hot Standby
Mode 4: Cold Shutdown	Mode 4: Hot Shutdown
Mode 5: Outage	Mode 5: Cold Shutdown
	Mode 6: Outage
Emergency situations such as fire, evacuation, medical, etc.	

The number of responders identified for each condition and state should be based on the minimal staffing levels. The number of extra responders for each shift may change significantly from day to day (illness, labor dispute, etc.), and the VA analyst should avoid using this higher number as the baseline planning number if it is not a required operational staffing level. Additionally, information on staffing levels and locations for the various conditions and states is useful in accurately modeling the response using mod/sim tools.

5.4.4.2 Response-issued Equipment

Individually assigned duty equipment for each post and patrol should be documented and kept current. The VA analyst should understand what equipment is available. The equipment information assists in accurately modeling the response. Some examples of duty equipment to document include:

- Type of vehicle (four-wheel drive; armored or non-armored, etc.)
- Weapon model and caliber
- Basic operational ammunition load and type of ammunition
- Chemical and biological weapons equipment (gas mask, etc.)
- Armored vest
- Radio
- Alternate communications (pagers, cellular telephones, site intercom, etc.)

- Night vision equipment
- Thermal imaging
- Breaching equipment
- Friend or foe identification equipment
- Weapons optics

5.4.4.3 Post and Patrol Orders

Post and patrol orders should be reviewed to understand and accurately characterize each post and patrol position. Information obtained from these orders provides the VA analyst with information to characterize how access controls are performed, how contraband detection is conducted, and how the response detects unauthorized activities: via an intrusion detection system, at a post on patrol, or in a guard tower. This data is used to model the response in computer-based modeling tools as well as in any of the tabletop methodologies.

5.4.4.4 Response Plans

Response plans detail the number of response personnel required to respond to a target, and the response assigned locations. During response characterization, these response plans are reviewed to determine expected responder actions and how command and control is implemented. The VA analyst should use these plans to determine which responder(s) are most likely to provide interruption and neutralization for a given adversary scenario and pathway. The VA analyst should also attempt to verify that the response team responds in accordance with the response plans during performance tests and normal operations.

5.4.4.5 Determining Alarm Assessment and Communication Time (AACT)

AACT FoMs are used to provide an accurate representation of the time required to assess and communicate an alarm situation for each identified protection layer (e.g., Owner-Controlled Area, PA, vital area). AACTs are established by performance testing and are separate from response force times.

The pool of data used for AACT determination includes performance testing of sensors and the central alarm station. The resulting data is then input into the modeling tools to provide an accurate representation of the assessment and communication used in determining the CDP for adversary pathways.

Using these data points, the AACT can be calculated using statistical analysis. One such analysis that captures the range of collected data would be a 75th percentile calculation. The following table provides an example of how AACT data can be collected using notional data.

Table 10: Examples of Assessment and Communication Times

PA - ALARM ASSESSMENT AND COMMUNICATION TIMES						
ALARM LOCATION	**ASSESSED BY**	**ACKNOWLEDGED BY POST/PATROL**	**ASSESS TIME (sec)**	**COMMO TIME (sec)**	**ACKNOW-LEDGEMENT TIME (sec)**	**TOTAL TIME (sec)**
Perimeter Intrusion Detection System (PIDS) Zone 1	CAS	P44	28	17	8	53
PIDS Zone 2	CAS	P12	33	14	6	54
PIDS Zone 3	CAS	P56	21	14	7	42
PIDS Zone 4	CAS	P56	26	18	6	50
PIDS Zone 5	CAS	P12	25	11	8	44
					AACT:	53
***No data here is representative of actual test data**						

5.4.5 Determining Response Force Time (RFT)

RFT is the time it takes the response to traverse to their predetermined positions, as identified in response plans, and to prepare to initiate interruption of the adversary's mission. RFTs are established by performance testing, including from LSPTs and FoF exercises.

Using collected performance testing data, the RFT can be calculated using statistical analyses, such as a 75th percentile calculation.

RFTs should account for:

- Type of equipment required for the response to respond
- Location of equipment
- Equipment donning time
- Responder travel time
- Any responder actions during travel (e.g., locking doors)
- Means of response movement
- Weapon preparation time
- Communication time
- Radio discipline
- Effects of radio jamming on response times

The following table provides an example of how RFT data can be collected, using notional data.

Table 11: Example of response force times

PA—PATROL 115 RESPONSE FORCE TIME					
RESPONSE MEMBER	**EQUIPMENT DONNING TIME (sec)**	**DISTANCE TRAVELTIME (sec)**	**WEAPONS PREPARATION TIME (sec)**	**COMMO TIME (sec)**	**TOTAL TIME (sec)**
P6	30	102	5	3	140
P6	21	102	8	5	136
P6	7	104	6	6	123
P6	13	107	8	5	133
P6	17	115	7	3	142
				75th PERCENTILE:	**140**
***No data here is representative of actual test data**					

5.4.6 Deadly Force Policy and Implementation

In addition to understanding the rules for using deadly force and site-specific rules of engagement as stipulated in policy, the analyst should also consider the site's deadly force training program to capture the nuances of implementing deadly force for a range of adversary actions. This task ensures that neutralization analyses are conducted in accordance with the actions that a response would take.

5.4.7 External Response Support

Site-specific agreements made with local law enforcement agencies should be reviewed if local law enforcement is used in determining P_E. This review should identify the agreed-upon required response time and the minimum number of law enforcement personnel to respond in an incident. The VA analyst should review documentation that verifies that the external agency:

- Is notified to respond in a manner that is understood by both parties
- Knows where to respond
- Understands the numbers and capabilities of the DBT
- Understands the target sets
- Is familiar with and has conducted a walkdown of the site and facility, structures and systems, plant hazards, and operations
- Has verified communications capability with the onsite response
- Has demonstrated, through past performance tests, the ability to perform as anticipated

5.4.8 Other Considerations

Other areas the analyst should evaluate to develop an accurate assessment of the response effectiveness in carrying out their mission are discussed below.

- **Picture in Time.** The site should conduct pictures in time based on unannounced observations of the response during different dayshift/on-shift and backshift conditions and target states. The purpose of conducting pictures in time is to gain data on the actual locations and readiness of the response force and patrols. In addition to characterizing the response, the information is used in system effectiveness analyses. It also provides some insight as to what the RFT could be for each post and patrol on a random basis. Capturing pictures in time regularly allows the VA analyst to understand the distributions of response force and patrol locations and readiness.

- **Shift Change.** An analysis should consider how response shift changes are conducted to determine the feasibility and impact of an adversary attack us during a shift change.

- **Building Evacuations in Response to Alarms.** One consideration is response procedures related to the roles and actions the response takes during a criticality evacuation or other full or partial building evacuation in response to alarms. These procedures should be reviewed to understand what measures are taken to verify that the alarm is not a false alarm, how occupants are controlled when evacuated, and what response presence or compensatory measures would be implemented during an evacuation.

- **Communications.** The ability to communicate effectively has a direct effect on detection, assessment, response times, and neutralization of the adversary. There are no default data for communications FoM. They are factored in when considering detection, assessment, and response. The site should determine the effects of jamming radio communications and to what degree response would be degraded. The site should also assess the knowledge and ability of the response to revert to alternate communications.

- **Ability to Neutralize Adversary Vehicles.** The analysis should evaluate the ability of the response to both interrupt and neutralize an adversary vehicle. This includes determining the operational weaponry deployed by the response.

- **FoF Configuration.** The analysis should evaluate the ability of the response to respond when in a FoF configuration if different from a normal configuration..

- **Validation and Verification of Response Characterization Information.** One of the most important aspects of ensuring the response characterization task is completed accurately is to validate and verify the FoMs that have been assigned to the various parts of the response operation that apply to detection, assessment, interdiction, and neutralization. Performance testing results should be used and incorporated into models.

5.5 Phase 3: Evaluate the PPS

Evaluating the effectiveness of a PPS involves conducting an analysis to determine how effective it performs against defined threats. Potential adversaries planning an attack have several options as illustrated in Figure 5, including scenarios in which they believe interaction with a response force is likely. In this case, they may select an attack scenario in which they preemptively attack the response force or attempt to divert the response force to increase their likelihood of success.

They may also attempt to prevent the response force from knowing to respond in the first place by an attack on the intrusion detection or communications systems in an attempt to prevent these systems from performing their functions. As PPS' become more and more computer-based, they potentially become vulnerable to cyber-attacks that may be attempted in conjunction with a physical attack.

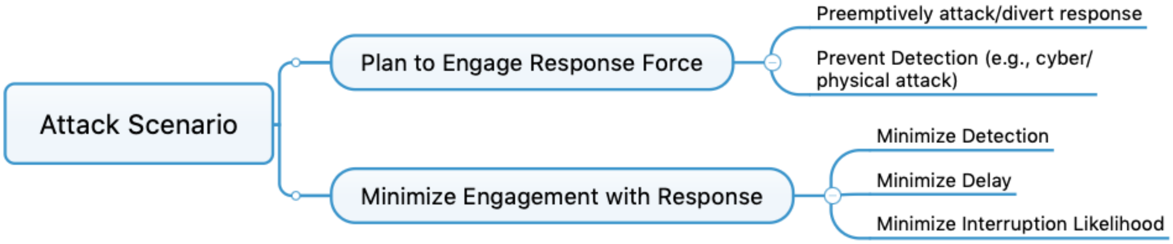

Attack Scenario
Plan to Engage Response Force
Preemptively attack/divert response
Prevent Detection (e.g., cyber/ physical attack)
Minimize Engagement with Response
Minimize Detection
Minimize Delay
Minimize Interruption Likelihood

Figure 5 - Attack Scenario Types

5.5.1 Evaluating Outsider Threats

Evaluating effectiveness of a PPS against outsider threats involves the conduct of path analyses, which evaluate the probability that a response force can interrupt adversaries whose objective is to minimize engagement with a response force; neutralization analyses, to determine the outcome of an engagement assuming interruption has occurred; and scenario analyses, where entire scenarios can be evaluated from the initial attack to the eventual outcome.

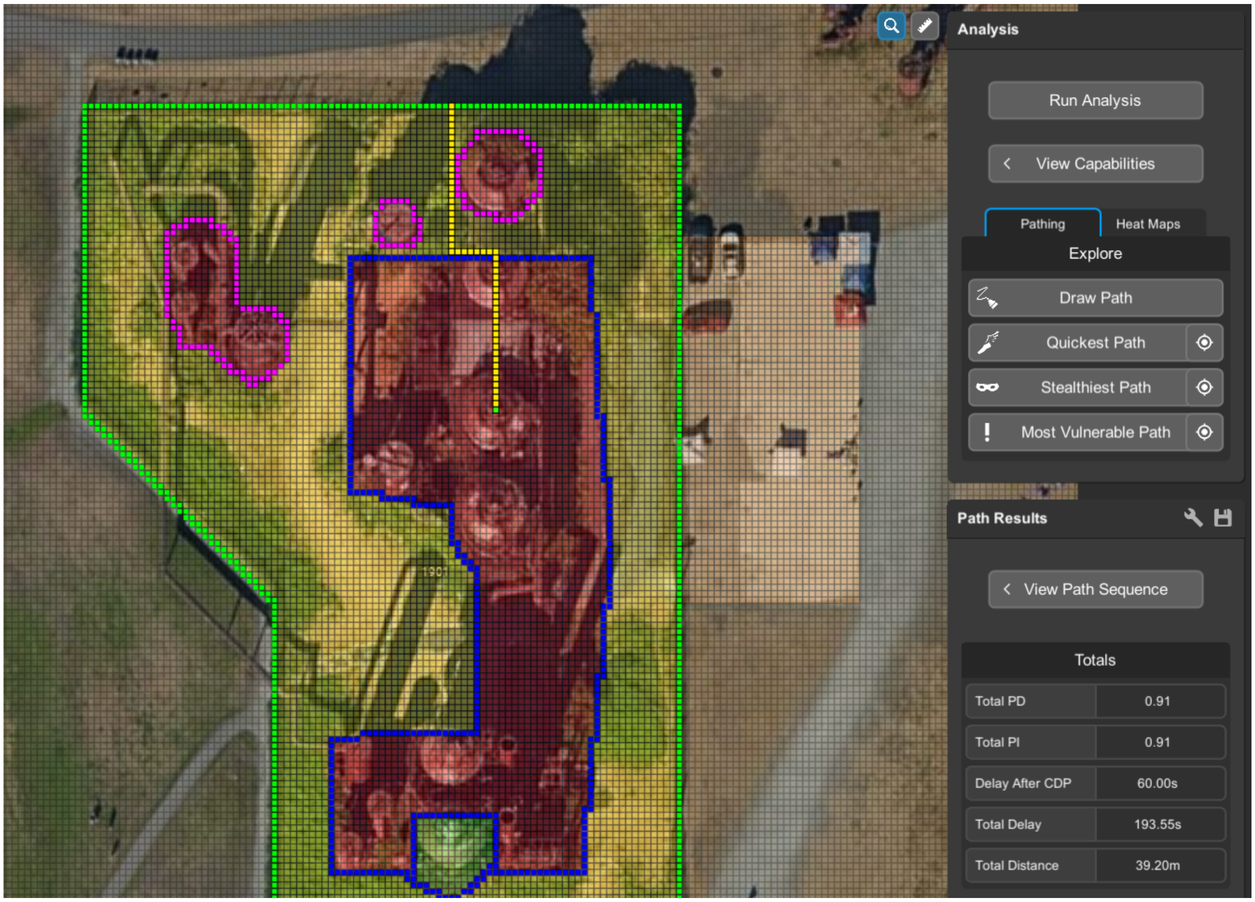
5.5.2 Pathway Analysis

To complete the objective of theft or sabotage, an adversary selects and follows some path from offsite to enter the nuclear facility and proceed to the theft or sabotage target; and, in the case of theft, the adversary also exits the site. This adversary path is defined both spatially and temporally, in terms of the physical route to the target and the time required passing along this route. This timeline also depends on the facility PPS, based on how the adversary chooses to avoid detection and penetrate barriers.

The PPS also has a timeline in response to the adversary actions. The timeline for the response is a function of system performance and includes times for detection, alarm communication, assessment, communication to the response force, and response force deployment. The relationship between the adversary and response force timelines determines whether the response force can interrupt the adversary before the theft or sabotage mission is completed.

The principle of timely detection is introduced to establish a quantitative metric for P_I. For the response force to be able to interrupt the adversary, it is vital that the PPS detects the adversary early enough along the adversary timeline that the response force has enough time to interrupt the adversary before theft or sabotage is completed. In this case, there is said to be timely detection of the adversary by the PPS. Without timely detection, the PPS is ineffective.

Government-owned mod/sim tools for pathway analysis include PathTrace, which allows for a rich design environment. Figure 6 shows an example screenshot of PathTrace.



Totals	
Total PD	0.91
Total PI	0.91
Delay After CDP	60.00s
Total Delay	193.55s
Total Distance	39.20m

Figure 6: Example pathway in PathTrace

Other tools perform a similar function and employ a 3D model of the site to automatically account for physical distances and the actual materials that define the barriers; this influences conditions such as the possibility of detection by a specific defender. Pathway tools should allow users to select available breaching tools (which help define the detection probability for barriers) and to specify the desired point where an adversary would transition from choosing a path that minimizes detection to one in which the adversary assumes detection would occur and therefore want to minimize time to the target(s). In all cases, once a model is created it can generate a series of pathways that, when sorted, yield the lowest probability of interruption using a user-provided response force time, barrier delay times, and site-specific and default P_D values.

Although pathway tools do play a role in identifying desirable adversary pathways, it is important to note all tools are limited by the data provided to the models. If schematics of underground pathways are not provided to vulnerability analysts and included in the models, then no tool could possibly identify a route using this axis of advance. Conducting a pathway analysis is more important when applied to new sites and to facilities still under design. For these cases, pathway tools can help to identify desirable pathways and allow vulnerability analysts to develop corresponding attack scenarios that exploit the pathway using tactics, techniques, tools, and weapons allowable by the DBT. Once again it is important to acknowledge that a pathway is not an attack scenario; it is simply the methods, and sometimes locations, used to move from an exterior point of no-detection to the target(s) that provides the defense the least opportunity to interdict the route.

The following sections discuss the process a VA analyst uses to conduct a pathway analysis.

5.5.3 Pathway Determination Process

To conduct any pathway analysis process, the analyst should establish a representation of the facility/site protective system. The analyst assembles FoMs into protection elements and layers that represent the protective system with the following considerations:

5.5.4 Protection Elements

The various FoMs determined from facility characterization and response force characterization are now grouped into protection elements or security elements that provide detection and/or delay. All viable facility/site protection elements that could be exploited by the adversary should be established so that all elements are considered in the pathway analysis process. As protection elements are established, all facility and response FoMs associated with each element should be identified. Each protection element should be uniquely named. The analyst may need to use multiple instances of the same element to describe the protective system more accurately. Possible protection element FoMs may include:

- **Boundary Barrier and Penetration Elements**
    - Surfaces (barriers, walls, floors, and roofs)
    - Windows
    - Ducts (penetrations above and below grade including heating, ventilation, and air conditioning penetrations)
    - Tunnels
    - Fence line

  - Isolation zone (e.g., PA)
  - Overpass (over buildings)

- **Entry/Exit Control Elements**
  - Personnel portal (human movement)
  - Vehicle portal (vehicle movement)
  - Shipping/receiving portal
  - Gateway (human and vehicle movement)
  - Door
  - Emergency exit

- **Adversary Sequence Diagram (ASD).** A schematic or visual diagram representation of a facility/site and its safeguards/security components. The ASD provides a way to consider all possible pathways. A completed ASD is also useful in ensuring that all elements and pathways can be considered.

- **Timely Detection.** Timely detection is a measurement of the interaction between the physical and human security components that detect a malevolent act in progress and barriers that delay adversaries long enough for the event to be communicated to a response force, who then deploys and interrupts the progress of the adversaries. The performance variables in this equation include detection probabilities (sensing and assessment), assessment time, communication time, adversary movement, barrier and other delay times, and RFT. Timely detection is the cumulative detection up to the point where the PF can respond in time to interrupt the adversary. This point is determined by the RFT. Some of the pathways relevant to timely detection determinations are the minimum delay pathway and the minimum detection pathway.
  - **Minimum Delay Pathway.** The minimum delay pathway is a process to evaluate the balance of delay systems at the site. This process is not used to calculate P_I but used to understand the delay FoM provided by barriers in the system. It may also be used to assist the analyst in scenario development. This methodology does not consider detection as part of the pathway determination.
  - **Minimized Detection Pathway.** Another process to evaluate the balance of detection systems at the site. This process is not used to calculate P_I but to understand the detection FoM provided by the intrusion detection capabilities of the protective system. It may also be used to assist in scenario development. This methodology does not consider delay as part of the pathway determination.

- **Evaluation of Results.** Many pathways are considered in pathway analysis, which includes the different types of pathways and the different target sets. If discrepancies exist where one or some pathways have lower P_I than the others, this may indicate that the PPS is unbalanced and vulnerabilities are present. In addition to P_I, the location of the CDP and the credibility of pathways are important considerations.
- **Element P_D.** P_D and delay times for each pathway element should be documented. When pathway elements are used in attack scenarios, these FoMs can be used as inputs to calculation of system effectiveness for that scenario. Note: P_E is determined from specific scenarios and not from any pathway analysis methods.

5.5.5 Scenario Analyses

P_E is estimated using sets of scenarios. A scenario is one method that adversaries can use to achieve their objective of theft or radiological sabotage. To perform this analysis, attack scenarios are developed, and then the scenarios are evaluated using models, simulations, tabletop methods, or FoF exercises. A scenario uses much more detail about how the adversary attack is conducted than just the path of the attack. It incorporates detailed information obtained from site security plans, procedures, and incident response plans. In addition, it requires developing detailed representative set of adversary scenarios/attack scenarios, which may involve potential collusion with insider threats.

5.5.6 Neutralization Analyses

P_N is a component of the overall effectiveness of a PPS, and measures the effectiveness of response given interruption. After interruption, the response force uses the force necessary to prevent the adversaries from completing their objective, which may require an armed engagement between the two sides.

P_N represents the likelihood of outcomes of engagements between adversary and response forces, but cannot predict the outcome of a single attack against a site. There are a number of methods used to measure P_N, and they require obtaining different types of data for use in an analysis.

Simple methods may only require data regarding the number of personnel and weapon types on either side, along with the time at which different numbers of each side are in an engagement. More complex models, such as simulations, may require a significant amount of data. Some examples include:

- Initial locations of response forces and adversaries
- Response force deployment routes and final locations
- Adversary path
- Adversary scenario
- Terrain

- Building schematics
- PPS characteristics (e.g., barrier delays)

Methods for determining P_N include performance testing, mathematical models, and simulations. Each method has its advantages and disadvantages, primarily in terms of time, cost, and accuracy. Some methods can analyze a few factors, while some can analyze many more. No method is able to account for all the factors that affect the outcome of a single engagement, but each can provide insight into the strength of a response force.

All methods are able to perform simple analyses from a small set of quantifiable data, such as the number of combatants on either side, the types of weapons used, and the response force time. Combined with SMEs to provide insights into data that can be qualitatively analyzed, these simple methods can be combined with expert judgment to account for other factors, such as the estimated number of response force casualties from a vehicle bomb detonated at an entry control point. The reduced response force numbers can then be used in the selected P_N method. Some factors are difficult to analyze with any method, such as tactical decisionmaking, morale, and casualties from non-combat events (e.g., response force members involved in a vehicle accident while responding).

5.5.6.1 Evaluating Insider Threats

Insider threats are challenging to analyze, but some similar methods used for evaluating outsider threats can be used for insider threats. The insider should be evaluated in a VA regardless of the use of an insider threat program.

5.5.7 System Effectiveness Methodology

Commercial nuclear facilities should use a more holistic or systemic approach as opposed to a layer-based approach. Using the holistic approach, a single analysis is conducted to determine the probability of security system effectiveness by incorporating the probabilities of detection, which typically inform a probability of interruption, directly into combat simulation and allow detection to occur as the scenario naturally dictates. This allows analysts to develop a single simulation that captures the adversary plan for a given scenario while allowing for the detection probabilities to drive when and where detection and assessment occurs. In some cases, based on P_D, the adversaries may traverse the feature, system, or layer undetected, and any detection later along the path would rely on subsequent adversary actions and detection capabilities. Using this approach, multiple valid statistical methods for calculating P_E could be utilized, but it is important to be consistent in the methodology used once one is selected.

This method preserves the effect of imperfect P_D on the system effectiveness yet yields a more straightforward assessment process that minimizes the number of attack scenarios developed and maintained, executed, analyzed, and accredited. Unlike layer-based processes, it also preserves the evolution of the detection process, especially in cases where deceit or some other form of deception is used by the adversary to gain access to a site. For any detection system that is less than perfect, which is to say all systems, the adversary has some probability of bypassing the system undetected and thus defenses rely on defense-in-depth principles to detect, assess, and neutralize the adversary.

This is not to suggest pathway analysis and the traditional computation of probability of interruption is not warranted or a valuable process, especially for new builds. P_I, determined using the response force time and critical detection point, should be used to evaluate and identify pathways or routes that are most advantageous to the adversary which in turn should inform the scenario development process.

5.5.7.1 Modeling and Simulation Tools to Produce System Effectiveness

Estimation of the probability of neutralization is more complicated than pathway analysis and is typically the driving factor in estimating P_E. While for most government sites and existing commercial nuclear operators P_I for delay and detection systems may be relatively high; in contrast, P_N can vary more widely based upon the defense strategy. It is imperative that any mod/sim tool used for neutralization assessment faithfully represents and uses the detection probabilities associated with the system and the defeat methods used by the adversary. Values should be based upon performance testing when possible, and in the case of new builds and plants under design one should use standard P_D values. However, to the extent possible, FoMs, including delay data, should be based on performance tests. This means FoMs used in mod/sim tools should reflect actual performance, and not an upper or lower threshold or *expected* performance values.

For combat analysis, it is critical to employ tools and data that are proven effective in representing the processes involved in attacking and defending the facility with sufficient fidelity to fairly characterize weapon engagements, breaching delays, explosive effects, exposure to weapons firing, detection systems, communication systems, and command and control elements. Modern mod/sim tools allow vulnerability analysts to create models of the facility, defense strategies and attack scenarios. These models are used in a combat simulation to essentially execute the attack scenarios in the context of a facility configuration, detection system and defense strategy. These scenarios include specific weapons, tools, barriers, vehicles, communications, and people using approved data to adjudicate weapon engagement and determine delay and detection opportunities. This simulates the FoF actions taken by an adversary as well as the defense's typically delayed reactions as knowledge of the adversary is discovered and distributed by the central alarm monitoring station or by individual defenders.

Equally important as the behavior models in a mod/sim tool is the use of accredited and vetted performance data. Specifically, the government-provided engagement data, frequently referred to as probability of hit/kill (P_H/P_K), is available for commercial nuclear operators. This data is available at a classification level appropriate for use by commercial operators. The data represents the likelihood of each trigger pull resulting in the target being neutralized for multiple weapon classes, munitions, distances, positions/movement status of shooter and target, etc.

To gain sufficient statistical data to compute P_E, several hundred executes should be run of each scenario. The resultant P_E values should incorporate statistically appropriate methods rather than just a raw wins/tests formula, and the calculated P_E should be less than 1.0. This limitation may initially prove disconcerting to traditional security professionals used to winning 100 % of the time in FoF drills; however, this process ensures a robust yet conservative approach that aligns with regulatory thresholds.

5.5.7.2 System Effectiveness Reporting

Individual P_E results should be reported for a given target. Multiple baseline scenarios are sound as a basis for system effectiveness determination. During this process, averaging P_E calculations from different scenarios is not an appropriate method. As adversaries can choose the scenario most advantageous to their mission, consideration should be given to the acceptance of scenarios with the lowest P_E.

5.6 Change Management

This process addresses activities to capture the operational configuration of a site in the VA. In addition, this process is designed such that all of the major activities associated with a VA—target identification and bounding, facility/protection system characterization, response force characterization, threat characterization, and finally neutralization analysis—are developed in accordance with policy.

A critical part of an effective VA program is a robust change management system. Such a system ensures that any proposed change within a facility made by any organization for whatever reason; whether of a structural, procedural, or organizational nature and whether temporary or permanent; is analyzed regarding their implications on the PPS and the VA. It is important that no reduction in the effectiveness of the PPS is allowed, even for short periods, without appropriate justification. If the change is short term, approved compensatory measures can be implemented. The change management system can also be used to protect against any proposed significant changes to the PPS that may compromise other systems, such as safety and emergency management.

Preferably, a defined management position should be appointed to approve each change, and the change should then be endorsed by those individuals whose area of responsibility is most affected. This review and approval process should be given particular importance when the activities which cause the change to be made are the responsibility of different parts of the organization. Evidence that the change satisfies VA and/or PPS requirements should be maintained.

Adequate monitoring as the change is implemented can provide early warning on any negative effects on PPS effectiveness, thereby providing sufficient time to take remedial action as necessary.

Examples of planned activities that could have a potential adverse impact on the PPS include:

- Activities to temporarily disable sections of a perimeter intrusion detection and assessment system during a refresh.
- Adding an addition to a building whose boundary is a defined security area.

5.7 Quality Assurance

VAs are very complex endeavors employing a wide range of FoMs along with other assumptions derived from a variety of sources. The validity of a VA depends on developing a detailed understanding of the facility and its protection systems and using accurate, well supported data.

6 A BEST PRACTICE FOR THE VA PROCESS: PERFORMANCE ASSURANCE PROGRAM

6.1 Purpose

Sites should have a performance assurance program (PAP) to demonstrate reliable, effective protection of site targets. To assist sites in verifying program effectiveness, it is recommended that sites conduct self-assessments and performance tests. To aid in accomplishing this, a comprehensive approach to the identification and testing of essential elements for security should be used.

Sites should implement and maintain a PAP in accordance with their overall protection goals that ensures essential elements used to protect site assets meet established requirements for reliability, operability, readiness, and performance prior to and during operation use. To meet these requirements, a comprehensive approach to identification and testing of essential elements for security assets should be used. Essential elements derived from the PAP process should be identified in security plans and procedures used to support vulnerability assessment reports.

6.1.1 Recommendations

PAPs should be tailored to address all assets at a site and be compromised of the total security system and safeguards and security programs. The PAP should tailor evaluation and testing activities at a site to ensure a systems approach to the evaluation of security programs. In addition, the PAP should provide a comprehensive approach to ensure an acceptable level of performance for identified essential elements of the site protection program crucial to system performance for all identified assets.

6.2 Performance Testing

An effective performance testing program provides both the reliability and assurance of security-related subsystems and components. The purpose of performance testing is to ensure systems, people, and procedures can perform as required, identify performance deficiencies, and support FoMs used in the vulnerability assessment for the protection of identified assets. Performance tests can range in complexity from simple demonstrations of component operability or single individual skill to major integrated tests involving an entire response shift operating with other elements of a facility's security system. Every performance test should be planned and conducted with the utmost regard to established safety standards and policies. While individual security components are tested to evaluate their performance, overall system effectiveness is evaluated using all systems present along an adversary pathway. Results from individual tests should be used in determining detection probabilities for an adversary pathway. When planning and conducting performance testing, the following should be considered:

1. All potential threat types and capabilities evaluation;

2. The adversary pathway and the equipment necessary to execute adversary objectives; and

3. All shifts and weather conditions testing.

6.2.1 Types of Performance Test

Performance testing should be used to realistically evaluate and verify the effectiveness of equipment, personnel, and processes; to identify and provide needed training; and to identify areas requiring system improvement. The types of performance testing that should be conducted include the following:

1. Limited Scope Performance Tests

    a. LSPT may be either scheduled or unannounced

        i. The tests should be used to determine the level of response force skill or capability or to verify different elements of the response force program

        ii. LSPTs should be conducted to realistically test any operation or procedure, verify the performance or a regulatory requirement, or verify the possession of a requisite knowledge or skill to perform a specific task that falls within the scope of the response force responsibility.

2. Alarm Response and Assessment Performance Tests

    a. ARAPT are conducted to evaluate the response force readiness and response to a specific location under alarm protection.

    b. These tests should consider all aspects or response including communications, individual and team tactics, decisionmaking, personal protective measures, equipment availability and serviceability, and any response and facility coordination activities that may be necessary to mitigate a security incident.

    c. ARAPT scenarios should be based on simulated adversary actions consistent with the NRC threat guidance and site-specific vulnerability assessments.

3. Force-on-Force

    a. The FoF is a major test to facilitate the assessment of all elements employed in response to DBT threats. The intent is to evaluate the response to malevolent events based on the adversary capabilities. The test should include both interior and exterior facility response.

    b. An FoF permits the site to evaluate the response force’s ability to interrupt and neutralize a DBT-based adversary under stressful, realistic conditions. In addition to providing valuable information about response capabilities, FoF exercises provide the opportunity to collect information and validate assumptions about response forces capability such as:

i. Knowledge and application of the use of force and rules of engagement

ii. The ability to communicate clearly and respond under stress

iii. Command and control

iv. The ability to distinguish between friendly and adversary activity under realistic conditions

v. Use of individual tactics and team tactics

vi. Effectiveness without a primary communication system

vii. Effectiveness of planned defensive positions and offensive tactics

viii. Use of cover and concealment

c. Additional Considerations:

i. Scenario objectives for FoFs should be based on the assessment of training, operational performance, and information derived from the vulnerability assessment.

ii. Baseline scenarios should be used for FoFs conducted for the purposes of evaluating the effectiveness of the protection strategy at a facility.

iii. The conduct of FoFs within operational facilities is optimal to minimize artificialities and maximize familiarity with targets.

4. Operability Test

Operability tests aim to determine if a given system element or group of elements (subsystem) of a PPS is functioning. It is important to note that operability tests typically do not determine how well the PPS is functioning, only whether the element is functional. Operability tests may find significant malfunctions or outages that should be immediately addressed with maintenance or via compensatory measures.

5. System Effectiveness Test

System effectiveness does not apply to any individual detection sensor but to all parts of the protection systems that work together in facilitating a response that mitigates the DBT adversary threat.

6.2.2 Determining Figures of Merit

Performance testing results should be used to determine FoMs used in the vulnerability assessment process. The preferred method for determining FoMs is to conduct a sufficient number of tests and use accepted statistical methods to achieve a 95 % confidence level. This is not possible in all cases. When an adequate number of test results are not available, the adjusted Wald interval method should be used to calculate a LOW value, a HIGH value, and a BEST ESTIMATE point estimation.

1. Testing data should be used to calculate a FoM and reported in a table similar to the example below.

2. This methodology may also be used to support essential element performance values.

Table 12: Example Performance Test Reporting Matrix

ELEMENT TESTED	TESTS	FAILURES	ADJUSTED WALD INTERVAL		
			LOW	HIGH	BEST ESTIMATE
Microwave Sensors	20	2	0.67	0.98	**0.86**
Active Sonic Sensors	16	5	0.44	0.86	**0.67**
Taut Wire Sensor	22	6	0.52	0.87	**0.71**
Capacitance Proximity Sensor	10	6	0.17	0.69	**0.42**
Note: No data here is representative of actual test data					

6.2.3 Weighting of Performance Test

Current fiscal year performance tests should be weighted higher than previous fiscal years in order to establish system performance trends and/or issues. For example, if using the current and previous years, the current year could be weighted at 60 % and the previous year at 40 %.

7 ADDITIONAL CONSIDERATIONS FOR A VA PROGRAM

7.1 Cost Considerations

Cost is a significant factor in any program. A process that is excessively cumbersome and fails to provide some form of savings or alleviation is unlikely to gain widespread acceptance. Furthermore, it is crucial that the developed process considers the broader implications for the site or asset that is being safeguarded.

7.2 Application of Insider Threats and Insider Mitigation Programs

A significant challenge lies in persuading sites to recognize the necessity of assessing threats posed by active insider adversaries, despite the existence of an approved insider mitigation program. This perspective is not widely acknowledged within the industry. Convincing industry stakeholders to consider these threats may prove difficult and could encounter considerable opposition. It is important to emphasize that while sites ought to evaluate such scenarios, they should not be regarded as baseline scenarios.

7.3 Established Physical Protection System Effectiveness Number

For sites intending to establish an analysis program, it is essential to consider a suitable system effectiveness metric against which the sites can evaluate their performance. This metric serves as a benchmark for acceptable levels of site protection. Additionally, it not only indicates compliance with established standards (e.g., regulatory standards), but it also aids in making informed decisions about capital enhancements or adjustments to security measures. It is crucial for sites to ensure that each scenario evaluated aligns with the defined performance effectiveness number, rather than relying on an average of multiple scenarios.

7.4 Program Rigor

Another important factor that deserves consideration is the degree of thoroughness required for implementing a vulnerability assessment process. This process necessitates that organizations implement a careful and methodical approach to security evaluations. The aim during these assessments should be to follow the established procedures while employing reliable performance data.

It is crucial to recognize that FoF data should be included in the vulnerability assessment; however, it should not serve as the sole input or focus. Some organizations attempt to align the outcomes of their simulations with the results and engagements observed in FoF evaluations by altering the inputs; this practice is not appropriate.

8 SUMMARY AND CONCLUSIONS

This report has provided a detailed examination of the VA process and the role of physical security mod/sim tools in enhancing the security of nuclear facilities. Through a comprehensive analysis of historical developments, current methodologies, and best practices, several key findings have emerged.

First, the transition from traditional layer-based approaches to a holistic framework for assessing PPSs has been identified as a critical advancement in the field. This new approach allows for the integration of detection probabilities directly into combat simulations, thereby providing a more accurate representation of adversary actions and the corresponding responses of PFs. By employing this methodology, analysts can better understand the dynamics of security systems and their effectiveness against a range of potential threats.

Second, the importance of robust PAPs has been emphasized. These programs ensure that essential elements of security systems are continuously evaluated and tested, thereby maintaining their reliability and effectiveness. The incorporation of self-assessments, performance tests, and regular updates to security measures is vital for adapting to evolving threats and ensuring continued compliance with regulatory standards.

Third, the report highlights the necessity of utilizing accredited mod/sim tools that accurately reflect the complexities of adversary behavior and the operational environment of nuclear facilities. The reliance on validated performance data is essential for establishing credible FoMs that inform vulnerability assessments and guide decisionmaking processes.

In conclusion, the findings of this report underscore the need for a systematic and integrated approach to vulnerability assessments in nuclear facilities. By leveraging advanced modeling techniques, conducting thorough performance evaluations, and maintaining a proactive stance toward security enhancements, stakeholders can significantly improve the resilience of their protective measures against potential adversarial actions. The ongoing commitment to refining the VA process ultimately contributes to a safer and more secure operational environment for nuclear facilities.

9 REFERENCES

[1] E. Cohn, J. Chang, J. Matrachisia and R. Iyengar, "Preliminary Assessment of Physical Protection Modeling and Simulation Tools ML23346A027," US Nuclear Regulatory Commission, Washington DC, 2023.

[2] M. L. Garcia, The Design and Evaluation of Physical Protection Systems, Burlington: Elsevier Butterworth-Herman, 2001.

[3] M. L. Garcia, Vulnerability Assessment of Physical Protection Systems, Albuquerque: Butterworth-Heinemann, 2006.

[4] D. McCorquodale and M. Talbot, "Using Fully Automated Comabat Simulation to Support Security by Design," in *Institute of Nuclear Material Management*, Albuquerque, 2023.

[5] J. Zamanali and C. Chwasz, "Nuclear Power Plant Security Assessment Guide NUREG/CR-7145," U.S. Nuclear Regulatory Commission, Washington DC, 2013.

[6] J. Helton, "Uncertainty and Sensitivity Analysis Techniques for Use in Performance Assessment for Radioactive Waste Disposal," *Reliability Engineering and System Safety,* vol. 42, no. 2-3, pp. 327-367, 1993.

[7] D. M. Hamby, "A Review of Techniques for Parameter Sensitivity Analysis of Environmental Models," *Environmental Monitoring and Assessment,* vol. 32, no. 2, pp. 135-154, 1994.

[8] H. C. Frey and S. R. Patil, "Identification and Review of Sensitivity Analysis Methods," *Risk Analysis,* vol. 22, no. 3, pp. 553-578, 2002.

[9] J. C. Helton, "Uncertainty and Sensitivity Analysis in the Presence of Stochastic and Subjective Uncertainty," *Journal of Statistical Computation and Simulation,* vol. 57, no. 1-4, pp. 3-76, 1997.

[10] J. C. Helton and D. E. Burmaster, "Guest Editorial:Treatment of Aleatory and Epistemic Uncertainty in Performance Assessments for Complex Systems," *Reliability Engineering and System Safety,* vol. 54, no. 2-3, pp. 91-94, 1996.

[11] M. E. Paté-Cornell, "Uncertainties in Risk Analysis: Six Levels of Treatment," *Reliability Engineering and System Safety,* vol. 54, no. 2-3, pp. 95-111, 1996.

[12] R. L. Winkler, "Uncertainty in Probabilistic Risk Assessment," *Reliability Engineering and System Safety,* vol. 54, no. 2-3, pp. 127-132, 1996.

[13] E. Hofer, "When to Separate Uncertainties and When Not to Separate," *Reliability Engineering and System Safety,* vol. 54, no. 2-3, pp. 113-118, 1996.

[14] G. W. Parry and P. W. Winter, "Characterization and Evaluation of Uncertainty in Probabilistic Risk Analysis," *Nuclear Safety,* vol. 22, no. 1, pp. 28-42, 1981.

[15] J. C. Helton, "Probability, Conditional Probability and Complementary Cumulative Distribution Functions in Performance Assessment for Radioactive Waste Disposal," *Reliability Engineering and System Safety ,* vol. 54, no. 2-3, pp. 145-163, 1996.

[16] F. O. Hoffman and J. S. Hammonds, "Propagation of Uncertainty in Risk Assessments: The Need to Distinguish Between Uncertainty Due to Lack of Knowledge and Uncertainty Due to Variability," *Risk Analysis,* vol. 14, no. 5, pp. 707-712, 1994.

[17] J. C. Helton, "Treatment of Uncertainty in Performance Assessments for Complex Systems," *Risk Analysis,* vol. 14, no. 4, pp. 483-511, 1994.

[18] G. Apostolakis, "the Concept of Probability in Safety Assessments of Technological Systems," *Science,* vol. 250, no. 4986, pp. 1359-1364, 1990.

[19] S. Kaplan and B. J. Garrick, "On the Quantitative Definition of Risk," *Risk Analysis,* vol. 1, no. 1, pp. 11-27, 1981.

[20] S. C. Hora and R. L. Iman, "Expert Opinion in Risk Analysis: The NUREG-1150 Methodology," *Nuclear Science and Engineering,* vol. 102, no. 4, pp. 323-331, 1989.

[21] M. A. Meyer and J. M. Booker, Eliciting and Analyzing Expert Judgment: A Practical Guide, New York: Academic Press, 1991.

[22] R. L. Keeney and D. V. Winterfeldt, "Eliciting Probabilities from Experts in Complex Technical Problems," *IEEE Transactions on Engineering Management,* vol. 38, no. 3, pp. 191-201, 1991.

[23] M. C. Thorne and M. R. Williams, "A Review of Expert Judgment Techniques with Reference to Nuclear Safety," *Progress in Nuclear Safety,* vol. 27, no. 2-3, pp. 83-254, 1992.

[24] M. C. Thorne, "The Use of Expert Opinion in Formulating Conceptual Models of Underground Disposal Systems and the Treatment of Associated Bias," *Reliability Engineering and System Safety,* vol. 42, no. 2-3, pp. 161-180, 1993.

[25] R. J. Budnitz and e. al., "Use of Technical Expert Panels: Applications to Probabilistic Seismic Hazard Analysis," *Risk Analysis,* vol. 18, no. 4, pp. 463-469, 1998.

[26] B. M. Ayyub, Elicitation of Expert Opinions for Uncertainty and Risks, Boca Raton: CRC Press, 2001.

[27] R. M. Cooke and L. J. Goossens, "Expert Judgment Elicitation for Risk Assessment of Critical Infrastructures," *Journal of Risk Research,* vol. 7, no. 6, pp. 643-656, 2004.

[28] R. Cooke, Experts in Uncertainty: Opinion and Subjective Probability in Science, New York: Oxford University Press, 1991.

[29] P. H. Garthwaite, J. B. Kadane and A. O'Hagan, "Statistical Methods for Eliciting Probability Distributions," *Journal of the American Statistical Association,* vol. 100, no. 470, pp. 680-700, 2005.

[30] G. Coles, J. Baweja and B. Jefferson, "Use of Expert Elicitation Guidance to Inform a Small-Scale Knowledge Judgment Application, RIL 2024-011," U.S. Nuclear Regulatory Commission, Washington DC, 2024.

[31] J. Xing and S. Morrow, "Guidance for Conducting Expert Elicitation in Risk-Informed Decisionmaking Activities, NUREG-2255," U.S. Nuclear Regulatory Commission, Washington DC, 2022.

[32] D. Brooks, A. Thompson and D. M. Osborn, "Risk-Informed Access Delay Timeline Development, SAND2020-9176," Sandia National Laboratories, Albuquerque, 2020.

[33] T. Noel, "Risk-Informed Timeline Tool, SAND2021-9430," Sandia National Laboratories, Albuquerque, 2021.

[34] Sandia National Laboratories, Lone Pine Nuclear Power Plant Hypothetical Facility Data Handbook SAND2021-2403 TR, Albuquerque: Sandia National Laboratories, 2021.