Letter Report
TLR-RES/DE/REB-2023-09

Preliminary Assessment of Physical Protection Modeling and Simulation Tools

December 2023

Brian Cohn
James Chang
John Matrachisia
Raj Iyengar
U.S. Nuclear Regulatory Commission

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

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Technical Letter Report

[TLR-RES/DE/REB-2023-09]

Preliminary Assessment of Physical Protection Modeling and Simulation Tools

Date:

[December 11, 2023]

Prepared in response to Informal Assistance Request "Preliminary Assessment of Physical Protection Modeling and Simulation Tools (White Paper)" [dated January 30, 2023], by:

Brian Cohn, John Matrachisia, Raj Iyengar
Reactor Engineering Branch

Division of Engineering

Y. James Chang
Human Factors & Reliability Branch

Division of Risk Analysis

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.

EXECUTIVE SUMMARY

This report provides a preliminary assessment of the state-of-technology of government-produced modeling and simulation (M&S) tools applicable to physical security and protection for nuclear facilities. This report examines M&S tools to identify the applications and limitations of the tools. The information in the report is aimed to prepare Office of Nuclear Security and Incident Response (NSIR) staff to review licensing actions using support from M&S tools. Additionally, this report will aid the development of regulatory guidance and inspection procedures for licensee use of physical protection M&S tools.

For this report, NSIR identified three government-produced M&S tools for the Office of Nuclear Regulatory Research (RES) to explore in the context of enabling Nuclear Regulatory Commission (NRC) staff to become familiar with computer-based security tools. Because physical protection M&S tools use similar approaches, the knowledge of these M&S tools can be applied to the NRC's oversight of those tools being used by industry. The functionality of each M&S tool, their physical protection applications, and their limitations are described in the report.

- Dante is a combat simulation tool which calculates the probability of neutralization and the probability of effectiveness for the site's physical protection system.
- Scribe3D facilitates tabletop exercises as a recording and visualization tool. Subject matter experts can view scenarios within a 3D model of a site and observe the consequences of changes at different points in a scenario to build a greater understanding of events during an attack.
- PathTrace supports pathway analysis by using a facility layout with detection and delay data to calculate the probability of detection and the probability of interruption for adversary pathways. The PathTrace tool can identify the stealthiest, quickest, and most vulnerable pathways to target locations.

The government-produced M&S tools have capabilities similar to the commercial M&S tools currently available. This scope of the effort was limited to these government-produced tools because the availability of the tools to NRC staff through no-fee licenses. Further, these tools enabled NRC-HQ staff to become familiar with computer-based security tools that focus on probability of interruption (P_I), probability of neutralization (P_N), probability of effectiveness (P_E), and tabletop exercises. The knowledge and insights gained with these tools will also be applicable to commercially available physical protection M&S tools. All physical security M&S tools, commercial and government-owned, will require realistic input data and accurate facility geometry to predict useful results. However, this report does not endorse any of the physical security M&S tools described herein.

Establishing in-house expertise with the government-produced M&S tools would support NRC headquarters staff's preparedness for licensing reviews of physical protection program designs and changes that are predicated on such tools, as well as associated oversight activities performed by regional inspectors. Because of the availability of government-owned tools, Dante, Scribe3D, and PathTrace, staff can utilize these tools to build capabilities and expertise by conducting an in-depth assessment of the tools, through use case demonstrations, and training.

CONTENTS

TABLES

ACRONYMS

LWRS	Light Water Reactor Sustainability
IAR	Informal Assistance Request
M&S	Modeling and simulation
NPP	Nuclear power plant
NRC	U.S. Nuclear Regulatory Commission
NSIR	Office of Nuclear Security and Incident Response
P_E	Probability of effectiveness
P_H	Probability of hit
P_I	Probability of interruption
P_K	Probability of kill
P_N	Probability of neutralization
RES	Office of Nuclear Regulatory Research
RESGC	NRC’s government cloud
SME	Subject matter expert
SNL	Sandia National Laboratories

1 INTRODUCTION

This Technical Letter Report provides information requested by the NSIR Informal Assistance Request (IAR) “Preliminary Assessment of Physical Protection Modeling and Simulation Tools (White Paper),” issued by NSIR/DPCP/MSB on January 30, 2023. That IAR seeks the following information related to three government-owned M&S software tools for physical security:

- Technical computer needs for the tools,
- Limitations and applications for the tools,
- Technical preparation for staff to review licensing actions utilizing physical protection M&S tools, and
- Recommendations for follow-on activities.

Staff identified three government-owned M&S tools for this initial assessment. The tools are Scribe3D, which facilitates tabletop exercises; PathTrace, which models attack paths; and Dante, which assesses the overall physical security system effectiveness. The scope of this effort was limited to these tools because the availability of the tools. Further, these tools enabled NRC-HQ staff to become familiar with computer-based security tools that focus on probability of interruption (P_I), probability of neutralization (P_N), probability of effectiveness (P_E), and tabletop exercises. The identified government-owned tools being explored have been made available to NRC staff through no-fee licenses.

Nuclear facilities (nuclear power plants and facilities that process special nuclear materials) are required to provide physical protection against sabotage or theft of nuclear material. Applicants and licensees may use vulnerability assessment methods:

- to design site physical protection systems, or
- confirm that either planned changes to their security plans do not decrease the safeguards effectiveness of those plans, or
- propose alternative security measures provide levels of protection equivalent to the prescribed measures they would be replacing.

Traditionally, vulnerability assessments are performed by a combination of hand calculations, exercises, and performance testing. However, software tools, including M&S, have been developed to support assessments that could aid effectiveness of security strategies. M&S tools can be used to support the identification of cost-effective modifications to the physical protection system while maintaining estimated or predicted system effectiveness. As a result, M&S tools have been used for physical security in the nuclear industry. NRC licensees have used commercial M&S tools, such as ARES Security Corporation’s AVERT [1] and RhinoCorps’ Simajin [2], to support changes to their security plans. NRC regulations require that changes to a facility’s security plans, unless accompanying a license amendment, not decrease the effectiveness of those security plans. Licensees' use of M&S tools has added to a technical basis for their determination that the security plan changes meet the NRC regulation.

Additionally, the Department of Energy's Light Water Reactor Sustainability (LWRS) program's physical protection pathway has taken a step forward on M&S by assessing the benefit of operator actions on reactor safety during hostile action-based events. LWRS has integrated reactor safety and physical security computer codes to model the sabotage scenarios to reactor systems in greater detail, including details about the timing of sabotage to reactor systems and of operator actions to prevent core damage. LWRS' study assessed the impacts of these timing effects and operator actions on reactor safety in sabotage scenarios [3].

It will be beneficial to develop NRC in-house knowledge and expertise on M&S tools to provide technical basis and support the development of potential future guidance for licensing or inspection. This in-house capability could improve the effectiveness of the headquarters staff and regional inspectors in evaluating the adequacy of the licensees' M&S results to justify the changes to the licensees' security plans.

2 OVERVIEW OF PHYSICAL PROTECTION

Physical protection for nuclear facilities is based on three primary elements: detection, delay, and response [4, 5]. A physical protection system is designed to *detect* adversaries with enough *delay* before those adversaries can achieve their goals to assemble a *response* that stops the adversary. A physical protection system's probability of effectiveness P_E is a measure of how well it performs these functions and is defined as

$$P_E = P_I \times P_N \qquad \text{Eq. 1}$$

where P_I is the probability of interruption, and P_N is the probability of neutralization given interruption. Interruption occurs when a response arrives at a time and in sufficient strength to require adversaries to pause their sabotage or theft tasks to engage with the response elements. Neutralization occurs when an adversary abandons the sabotage or theft tasks completely due to being driven off, made to surrender, or killed. Neutralization of the adversary ends the security portion of an M&S scenario.

P_E can be used by licensees to provide a technical justification that their physical security programs, as detailed in their security plans, provide high assurance[*] that their activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety. This assurance is a requirement under 10 CFR Part 73, and under 10 CFR 50.54(p), licensees cannot make changes to the security plans that rely on alternative measures or decrease their effectiveness without amending their licenses.

There are several evaluation processes that contribute to the calculation of P_I and P_N. These processes can be divided into several broad categories:

- Hand calculations,
- Drills and exercises, including limited scope performance testing,
- Subject matter expert (SME) opinion, and
- Computer M&S.

[*] The general performance objective of 10 CFR 73.55(b)(1) is to provide "high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety." In SRM-SECY-16-0073, Options and Recommendations for the Force-on-Force Inspection Program in Response to SRM-SECY-14-0088, the Commission stated that "the concept of 'high assurance' of adequate protection found in our security regulations is equivalent to 'reasonable assurance' when it comes to determining what level of regulation is appropriate" (ADAMS Accession No. ML16279A345).

For all processes, the calculation of P_I depends on the adversary's attack pathway. As an adversary travels through a facility toward a target, they will cross into and through several detection points, such as areas of sensor coverage, alarmed doors, or guard patrol routes. Each of these detection points has an associated probability of detection based on whether or how an adversary attempts to defeat the sensor and the licensee's ability to assess intrusions when they are sensed. P_I is the probability that adversaries are detected at any of these points with enough remaining delay time for the nuclear power plant (NPP) facility's response to interrupt the adversary.

P_N is the probability that the security force will successfully defeat the adversaries, given interruption. There are multiple ways to calculate P_N. Hand calculations to estimate P_N are of limited utility and would be more likely obtained from SMEs. Exercises attempt to capture the complexities of engagements, and either calculate P_N or provide information to assist expert elicitation. Tabletop exercises are discussion-based events that often use "probability of hit" (P_H) and "probability of kill" (P_K) tables to estimate P_N. The assessors determine the hits and kills using generally accepted probability tables that account for distance, weapon type, level of training, etc. Drills and exercises have people perform actions expected of adversaries and response forces in a simulated manner to estimate P_N by tracking the actions performed and their outcomes. The multiple forms that drills and exercises include are:

- Tabletop exercises, where SMEs use structured discussions to explore a site's physical protection system,
- Limited scope performance tests, where a small number of aspects of a site's security plans, such as individual adversary tasks or security components, are tested in isolation, and
- Force-on-force exercises, where a simulated adversary attempts to attack a facility and engages with all elements of that facility's physical protection system.

Vulnerability assessment is a structured process to estimate P_E. This process involves the development of adversary attack scenarios and evaluates the results of force-on-force engagements between adversaries and response forces in these scenarios. For vulnerability assessments, a scenario describes a set of adversary and protective capabilities along with an adversary attack pathway and objective. The process for performing vulnerability assessments involves several drills or force-on-force exercises, which can have notable challenges, including cost, safety considerations, and artificialities.

While limited scope performance tests, tabletop exercises, and force-on-force exercises provide valuable data for vulnerability assessments, they are not able to provide details of how the data captured from a drill or performance test integrates into a scenario as a whole. For example, a performance test may capture the time necessary to breach a fence as an adversary task. However, such a test would not capture the probability of detection for adversaries breaching that fence in its installed location. Additionally, the test would not account for factors affecting the performance and reliability of adversaries and security force when performing that task as part of a complete scenario (e.g., being under fire). These may affect the breaching time obtained from the earlier performance test. Depending on the specifics of the scenario under consideration, these additional factors may make the scenario that requires breaching the fence nonviable. For example, consider a fence that is sufficiently well defended. Attempting to breach it would lead to the defeat of the adversary force. In such a situation, the adversaries would choose a different route to be successful, even if the time to breach the fence is short. For these reasons, force-on-force exercises and physical security M&S tools are complementary and can provide a reliable assessment of a physical protection system.

Review by SMEs is one method that is used to identify insights from exercises and vulnerability assessment evaluations. While the details of events that occur during an adversary attack are uncertain, there are certain bounds of plausibility for these events. An SME that understands the adversary's capabilities can review the simulation results to determine the validity of the simulated scenarios. This allows the expert to not only consider if the individual events within one scenario are credible, but also if the combination of events that makes up a scenario is credible (e.g., ensuring simulated adversaries are protecting and recovering specialized assets that are needed for later tasks).

3 MODELING AND SIMULATION FOR PHYSICAL PROTECTION

Over the last several years, M&S tools have been used by NPPs to address some of the challenges associated with assessing P_E. While P_I can often be found through hand calculations, finding P_N is not suited for straightforward mathematical formulas. Instead, calculating P_N is a major function of many M&S tools, which have been developed to assist in several parts of the physical protection evaluation process in both the commercial and the government spaces, though some of these tools are also able to calculate P_I.

As computer codes, M&S tools use a combination of boundary conditions and initial conditions, where initial conditions describe events occurring within a scenario and boundary conditions are constraints that the simulation operates in. For physical security M&S, examples of boundary conditions would include adversary capabilities and the site layout. Examples of initial conditions would be the adversary pathway and the protective strategy.

AVERT and Simajin are examples of commercially available M&S tools which calculate P_N by simulating a force-on-force scenario many times to generate neutralization statistics, with each simulation of the scenario being a realization.

An additional benefit of using M&S tools is that, as digital files, simulations of a scenario are recorded in their entirety and can be copied with no loss of detail. This may ease staff's review of licensee submittals and could potentially reduce the cost burden of meeting regulatory requirements.

Sandia National Laboratories (SNL) has created several government-owned software tools to assess physical security effectiveness that may be relevant to the NRC. This report describes three of these tools:

- Dante,
- Scribe3D, and
- PathTrace.

3.1 Dante

Dante is a physical security suite that performs force-on-force simulations using an agent-based approach. Dante simulations generally model an attack scenario, which involves adversary agents moving through a 3D model of the site to reach an objective or set of objectives, based on a defined adversary pathway, guarded by a defensive team of agents, whose behavior is controlled by the response force strategy. Dante simulates many realizations of the attack scenario to calculate P_N, which is based on the successes or failures of the response force to prevent adversaries from achieving their objectives.

The modeling of agents in Dante is done through its simulation engine. Agents (adversaries and security forces) are given specific tasks to perform, such as moving to a waypoint. The tasks describe larger activities while specific behaviors of the agents are governed by a behavioral model. This model allows the simulation engine to insert additional actions and change the prioritization of actions based on circumstances. For example, if an agent is under fire, the agent may change their actions to running to cover and returning fire. Such behavior is governed by the rules set of the behavior model. This allows the analyst to model a scenario without needing to precisely plan each entity's responses to possible events which might occur.

The Dante simulation results contain the entirety of the data generated by the simulation, which can be explored by using inbuilt analysis tools. The Dante output can be interrogated in several ways beyond the topline results. These include generating death plots showing the location of deaths for a scenario or tracking the actions performed by agents. Statistical distributions showing who killed whom for several realizations of a scenario, or over several distinct scenarios, can provide useful data in determining the effectiveness of the current protective strategy and a means to assess 'what if' scenarios.

3.2 Scribe3D

Scribe3D is a tabletop recording and visualization tool. It is not intended to operate at the same level of fidelity as Dante nor to directly calculate P_N. Instead, Scribe3D is used in a human-in-the-loop fashion to create and record scenarios developed from tabletop exercises. During this mode of operation, Scribe3D uses a 3D site model and agents to replace the 2D map and figures that are often used in tabletop exercises.

Agents in Scribe3D are designed to be quick to place and control, such that an analyst controlling a Scribe3D scenario can construct and continue a scenario alongside participants in a tabletop exercise. As such, agents in Scribe3D do not have behaviors beyond what the analyst inputs. While analysts can choose between an agent traveling directly to a waypoint or following the terrain, the agent will proceed to the waypoint on the exact chosen route and ignore other activity, such as ongoing engagements.

Furthermore, as a recorder for tabletop exercises, Scribe3D is deterministic apart from depending on probability of hit/probability of kill tables to model weapon effects. Scribe3D scenarios can be rolled forwards and backwards in time at different speeds, as well as set to a specific time in the scenario. Scribe3D can further be used to address 'what if' questions or facilitate SME discussion by copying a scenario to an earlier time and proceeding differently. Scribe3D scenarios can be viewed in 2D, 3D, in first person from any agent, or as a set of transcripts to enable easier discussion and understanding of events.

3.3 PathTrace

PathTrace is a 2D tool that automates finding the fastest, stealthiest, or most vulnerable attack pathways to a set of target locations within a facility, as well as modeling any analyst-defined pathway. This tool may also allow investigation of other attack pathway strategies. PathTrace is a fully deterministic code which uses detection and delay data to model adversary pathways through a site. The purpose of this tool is to aid analysts in determining P_I.

In a PathTrace model, the site is divided into cells, where each cell has the makeup of the contents of its location (e.g., a wall, a door, or a hallway). The analyst assigns delay times and detection probabilities for entering the cell, based on its makeup. For example, entering a reinforced wall cell can have a delay time of 100 seconds and a detection probability of 50%, while entering a detection coverage zone is assigned a delay time of 0 seconds and a detection probability of 90%. All pathways between adjacent cells from the outside of the site to the targets are calculated. The pathway with the minimum delay time and the minimum probability of detection are automatically reported from this information, though analysts can also specify pathways to model. An additional input into PathTrace can be the response time. With this information, PathTrace can identify the most vulnerable path to the protective force strategy and calculate P_I for that path.

3.4 Input Requirements and Capabilities

The three computer codes described in this report each have different purposes and outputs. Similarly, each of the three codes require slightly different input data. Some of the data required by these codes is required for existing vulnerability assessment methods. For example, the probabilities of detection for sensors at a site are included in the calculation of P_I, for both hand calculations and M&S. A summary of the inputs for M&S codes is given in Table 1. For all three codes, realistic inputs and accurate facility geometry are generally required to predict useful results.

Table 1 Necessary inputs for selected M&S tools

	Dante	Scribe3D	PathTrace
2D Layout	N	N	Y
3D Site Model	Y	Y	N
Target Sets	Y	N	Y
Adversary & Response Numbers	Y	Y	N
Adversary & Response Capabilities	Y	Y	N
Site Physical Protection Data	Y	N	Y
Adversary Traversal & Delay Times	Y	Y	Y
Adversary & Response Strategy	Y	N	N

Dante is a code that simulates force-on-force engagements without a human-in-the-loop. Dante tracks the adversary pathway through the facility to their objective and the response force's actions. The tactics and policies of a facility define rules and priorities for the response force's actions, which are interpreted and applied by Dante during a simulation. Human behavior models are similarly used to determine what is known by agents and can interrupt actions an entity is taking with higher priority actions, allowing for agents to react to developments during an attack rather than following a set of scripted actions. The boundary conditions and initial conditions required for Dante to simulate an attack scenario are specified in Table 1. The 3D site model defines the physical geometry of the space that agents move through, and additional scenario data including the target sets, traversal and delay times, numbers, capabilities, and strategy of the adversary are used to describe the adversary's tactics and movements during the simulated attack. The response numbers, readiness and traversal times, capabilities, and strategy describe how the licensee intends to protect the site against the modeled attack. All of the information is used to perform a full-scope force-on-force simulation. The process of collecting the necessary models and data, as well as building the scenarios, requires a significant degree of effort to construct. However, when modeling limited scope actions, such as modeling adversary travel through a portion of the protected area fence, Dante only requires the input data needed to simulate the activities of the limited scope.

Scribe3D is primarily designed to function as a tabletop recorder. In this mode, Scribe3D runs as a human-in-the-loop simulator, which allows analysts to use one initial setup and progress events during the scenario based on expert input. An example of this would have one set of experts controlling adversary actions while a separate set of experts controls response force actions. Running in this mode, SMEs view the information that is available to them and decide how their side would respond. These actions are entered into Scribe3D, which implements the scripted actions and presents the updated scenario back to the SMEs for further decisions. The 3D model defines the space for the scenario, and the other input data described in Table 1, as necessary, defines the starting parameters of a scenario. Numbers and capabilities of adversaries and response forces are required to properly set up agents for a scenario, including their equipment and starting locations. Finally, traversal and delay time information is required to build appropriate movement speeds into the agents and be able to appropriately model adversary breaching activities. Strategies and target sets are not shown as required inputs because, as a tabletop recorder, these are often sourced from SMEs for an exercise. One Scribe3D model can be used to model a wide variety of scenarios.

PathTrace models potential adversary pathways and has correspondingly different uses and data requirements from Dante and Scribe3D. The intended use of PathTrace is to assist pathway analysis by modeling adversary movements through a facility. This can either be by exploring the timing and probability of detection for a specific path of interest, or by automatically identifying pathways of interest. This analysis of pathways, however, does not include interactions between adversaries and response forces. PathTrace requires 2D layouts of the simulated site. Multiple layouts are connected to model several levels of the 3D structures. To develop minimal delay and minimal probability of detection pathways, the corresponding site data is required. This includes the target locations, probabilities of detection for sensors, delay information, and traversal times. In addition, the response time can be included in PathTrace. This is a single number that describes the time following initial detection that it takes to deploy the response forces and intercept the adversaries.

4 USE-CASES FOR MODELING AND SIMULATION TOOLS

Using M&S tools can provide analysts with information that can serve as part of the technical basis for assessing the effectiveness of a licensee's physical protection system. In addition, the relative ease of developing 'what if' scenarios allows analysts to explore a wide variety of modifications to their physical protection system. Using M&S, analysts evaluate the effects on the security system from changes to protective strategies, physical barriers, facility layout, and available equipment. Licensees can use this function to develop a cost-effective way to maintain adequate protection. However, the raw output of an M&S tool is not enough information to make those determinations. Appropriate postprocessing and analysis work, and performance-based testing, need to be performed to validate and verify the results produced by M&S tools.

This paragraph discusses a real-world example of using an M&S tool to support changes to a physical protection system. Modeling of a site determined that adversaries had a high probability of evading detection when entering through the personnel portal by using false credentials. This adversary pathway reduced the site's P_E to an unacceptably low level. As a result, the site altered its access control system in the personnel portal, adding turnstiles and three-factor identification. The changes significantly improved the probability of detection in the personnel portal. The site re-evaluated its physical protection system following the upgrade implementation and then found that adversary penetration through the double-fenced protected area isolation zone became the most effective adversary pathway. An M&S tool analyzed this pathway. The results showed that the security guards did not have sufficient time to interrupt the adversary because of where they were routinely positioned in the perimeter towers. Adversaries could exit the line of sight of the perimeter towers before the stationed guards had time to receive the alarm, ready their weapons, and provide accurate fire. Based on these results, a change to the physical protection system by redeploying the guards from the perimeter towers closer to the target location was proposed and evaluated by using M&S tools. For this changed system M&S tools showed a high P_E. Limited scope performance tests and force-on-force exercises were used to confirm that the M&S results were credible and should be implemented.

One major limitation with all methods that calculate P_E is that the obtained value is specific to the analyzed scenario. P_E represents the likelihood of interruption and neutralization of a specific set of adversaries following a specific set of tasks by a given response strategy. Different adversary attack paths (e.g., entering from the south instead of the east) will often have different values for P_E. Therefore, a P_E is specific to an attack scenario. The effectiveness of a physical protection system should be represented by separate P_E values spanning the gamut of credible attack scenarios instead of using an averaged value for P_E.

Expertise is needed at every stage of calculating P_E, including developing attack scenarios, identifying assumptions and input parameters, running the simulations, and postprocessing the output of an M&S analysis. As P_E is specific to an attack scenario, proper scenario selection is necessary to ensure sufficient coverage of the scenarios of interest (e.g., assessing a worstcase scenario) and justify the design basis threat elements and attack strategies used for the scenario scheme.

The process of developing and running scenarios is similarly challenging. When building out a scenario, an analyst needs to make an informed decision about the values of parameters. For example, in Scribe3D, the analyst chooses the precise location that each adversary takes when conducting a breach and covering the breacher. These decisions affect simulation results. In some situations, their impacts may cause the events of a scenario to deviate from the SMEs' expectations. Therefore, the M&S output needs to be reviewed by the analyst and SMEs to identify aberrant behavior or inaccurate depictions of scenario play.

Validating M&S tools and their correct use by facilities require understanding of the tools, including modeling capabilities and input data. As applicants or licensees design their facility security plans and use M&S tools to contribute to their technical basis, NRC in-house expertise in the M&S tools would enable NRC headquarters staff and regional inspectors to more efficiently review licensees' submittals that involve the use of M&S tools.

5 ANSWERS TO IAR QUESTIONS

This section provides direct answers to the five questions asked in the IAR.

Q1. What are the technical computer needs for the tools?

Answer: Each of the M&S tools run on MS Windows systems, but the resources required depends on the tool. PathTrace does not use 3D models and can operate with limited resources. Scribe3D and Dante require additional resources, including graphics capabilities, due to their use of 3D models. The NRC's government cloud (RESGC) allows NRC staff to rent high performance virtual computers and pay the fee based on the duration of usage and the computation power. The RESGC can be an alternative to install the M&S tools instead of purchasing a physical computer, but this alternative may not be viable when modeling real facilities, due to the need to limit modeling to computer systems appropriate for processing safeguards information for NPP analysis and classified information for Cat I special nuclear material facilities.

Q2. What are the limitations and applications for the tools?

Answer: Every tool has its limitations. Common to all three codes, realistic input data and accurate facility geometry are necessary to produce useful predictions. Additionally, each of the three codes has different areas where they are most effective. PathTrace was developed as a pathway analysis tool and is not able to model interactions between adversaries and response forces. In addition, more unconventional pathways may not be identifiable without specific additions to the model to include them.

Scribe3D is primarily intended for use as a tabletop recorder and is applicable for those and similar tasks, including scenario development. Its neutralization simulation capabilities are limited due to its lack of automation of agent actions. As such, Scribe3D is limited in its ability to operate in a human-out-of-the-loop fashion.

Dante models have been used to support P_N calculations for scenarios. However, the complexity of constructing Dante models reduces their ability to make rapid changes to a model or to build a large number of models. As such, it is not often used to support scenario development activities.

Q3. Can M&S tools be appropriately used for physical security for NRC-licensed Category I special nuclear material facilities and nuclear power plants?

Answer: NRC NPP licensees have used commercial M&S tools to support security plan changes. M&S tools are typically accredited to analyze one or more of six functional areas: (1) facility characterization, (2) pathway analysis, (3) combat simulation, (4) system effectiveness, (5) upgrade analysis, and (6) cost-benefit analysis. M&S tools can be appropriately used for

NRC-licensed Category I special nuclear material facilities and NPPs in the accredited functional area(s).

Q4. How would M&S tools enable the NSIR staff to review licensing actions when supported by physical protection M&S tools?

Answer: Licensees and potential applicants have already begun using physical protection M&S tools to support updates to and the design of physical protection systems. Familiarity with the types of physical protection M&S tools available and their applications, capabilities, inputs, outputs, settings, limitations, uncertainty, and best practices can assist NSIR staff to effectively and efficiently review licensee's submittals that involve the use of physical protection M&S tools. This knowledge can be used by NRC headquarters staff to develop training materials to support regional inspectors.

The processes for developing physical protection M&S analyses depend on the application of the M&S tool being used. For example, pathway analysis requires data on the cost of adversaries taking different routes or performing different tasks to achieve their objective. However, there are also decisions that need to be made by the analyst that may have some effect on the model output. A specific example of this would be an analyst choosing different mesh sizes for the facility. This parameter affects movement through the plant and model performance. Because the government-owned physical protection M&S tools serve the same purpose as some of the commercially available tools, the insights gained from the government-owned tools could directly support staff reviews of licensee submittals and how they integrated the use of commercially available tools. In-house training can give inspectors an understanding of processes and modeling decisions to address physical security M&S.

Q5. What are the recommendations for follow-on activities?

The NRC's licensees have used M&S tools for their regulatory applications. The staff recommends to enhance the in-house expertise with government-owned M&S tools to support NSIR's headquarters staff's preparedness for licensing reviews of physical protection program designs and changes that are predicated on such tools, as well as associated oversight activities performed by regional inspectors. Expertise with these tools could also be leveraged to more efficiently cross-train with commercially available physical security M&S tools.

6 SUMMARY AND CONCLUSIONS

Nuclear facilities are using M&S tools to provide a technical basis for modifications to security plans. Prospective applicants for new or advanced reactors are also using M&S tools to design and test conceptual physical protection plans and elements. The use of M&S is intended to support a technical justification that (1) the changes made by facilities meet NRC regulations (i.e., 10 CFR50.54(p)(2), 10 CFR 50.90, 10 CFR 70.32(e), and 10 CFR 70.34) on the effectiveness of the security plans, (2) proposed alternative security measures provide levels of protection equivalent to the prescribed measures they would be replacing, and (3) physical security program or element designs would reasonably be expected to meet the physical security requirements in 10 CFR 73.55 or the proposed 10 CFR 73.100. To accomplish this, sites are leveraging these tools to estimate P_I, P_N, and P_E for scenarios of interest.

Utilization of M&S tools reduces the need for facilities to perform hand calculations when estimating P_I, supports the estimation of P_N alongside drills and exercises and provides a calculation of the probability of physical security system effectiveness. M&S tools can model a facility at a high fidelity to reduce the reliance on conservative assumptions when modeling scenarios. M&S can also generate a large volume of reproducible data for analysts to interrogate scenarios of interest. This aspect of M&S dovetails with the challenges when performing drills and exercises, allowing for a more complete understanding of the effectiveness of a facility's security plans.

Developing NRC in-house expertise with physical protection M&S tools would (1) support the development of potential future guidance for licensing or inspection, (2) provide NRC staff expertise to inform staff's review of licensee submittals and regional staff's inspections conducted, and (3) support NRC in being a modern risk-informed regulator.

7 REFERENCES

[1] ARES Security Corporation. *AVERT*. 2019; https://aressecuritycorp.com/software.

[2] RhinoCorps. *Simajin*. 2019; https://www.rhinocorps.com/products/simulation-application-suite/.

[3] Christian, R., S.R. Prescott, V. Yadav, S.W. St Germain, and J. Weathersby, *Light Water Reactor Sustainability Program - Methodology and Application of Physical Security Effectiveness Based on Dynamic Force-on-Force Modeling*, 2020, INL/EXT-20-59891, Idaho National Laboratory, https://lwrs.inl.gov/Physical%20Security/Methodology_Application_Physical_Effectiveness_based_on_FoF.pdf.

[4] Garcia, M.L., *The Design and Evaluation of Physical Protection Systems*. 2001, Elsevier Butterworth-Heinemann.

[5] Garcia, M.L., *Vulnerability Assessment of Physical Protection Systems*. 2006, Elsevier Butterworth-Heinemann.0-7506-7788-0.