INL/RPT-25-86929

Light Water Reactor Sustainability Program

A Comparison of Data from Physical Security Simulation Tools for use in MASS-DEF Optimization

August 2025

U.S. Department of Energy

Office of Nuclear Energy

INL/RPT-25-86929

A Comparison of Data from Physical Security Simulation Tools for use in MASS-DEF Optimization

Steven R. Prescott
Robby Christian
Shawn W. St Germain

August 2025

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

Page intentionally left blank

SUMMARY

The requirements for U.S. nuclear power plants to maintain a large onsite physical security force contribute to their high operational costs. The cost of maintaining the current physical security posture is approximately 10% of the overall operation and maintenance budget for commercial nuclear power plants. The goal of the Light Water Reactor Sustainability (LWRS) program's physical security pathway is to develop tools, methods, and technologies and provide the technical basis for an optimized physical security posture. Work under this program has shown that conservatism built into current security postures may be analyzed and minimized to reduce security costs while still ensuring adequate security and operational safety. Earlier research performed at Idaho National Laboratory within LWRS program's physical security pathway has successfully developed and demonstrated dynamic force-on-force modeling framework using various computer simulation tools and integrating them with the dynamic assessment Event Modeling Risk Assessment using Linked Diagrams (EMRALD) tool. This integrated process for physical security analysis is named Modeling and Analysis for Safety Security using Dynamic EMRALD Framework (MASS-DEF).

Nuclear power utilities in the United States typically use one of two commercial vendors software tools, RhinoCorps' Simajin or ARES Security's AVERT, for physical security modeling and simulation. As the MASS-DEF process couples with physical simulation tool result output, their results can have significant impact on the overall results of the optimization. This research has compared the results of these two software tools and how that data feeds into the MASS-DEF process. Results show that while the two software tools have similar overall outcomes for attack scenarios, there can be significant differences in the time required for adversaries to achieve their objectives due to multiple factors all of which can impact modeling tools that use those timing results.

Note that this report only provides comparison data and does not contain specific modeling results as those contain sensitive security information. No plant sensitive information and/or safeguards information is included.

Page intentionally left blank

CONTENTS

FIGURES

TABLES

Page intentionally left blank

ACRONYMS

CCDP	Conditional core damage probability
DBT	Design Basis Threat
DOE	Department of Energy
EMRALD	Event Modeling Risk Assessment using Linked Diagrams
FLEX	diverse and flexible mitigation capability
IAEA	International Atomic Energy Agency
INL	Idaho National Laboratory
LWRS	Light Water Reactor Sustainability
MAAP	Modular Accident Analysis Program
MASS-DEF	Modeling and Analysis for Safety and Security using Dynamic EMRALD Framework
MODSIM	Modeling and Simulation
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
O&M	operation and management
PE	Probability of Effectiveness
PN	Probability of Neutralization
PPS	Physical protection system
RAPT	Reasonable Assurance of Protection Time
SGI	safeguards information
UI	User interface

Page intentionally left blank

An Evaluation of the Dynamic Physical Security Risk Assessment Methodology for Fleet-Wide Applications

1. INTRODUCTION

Operation and maintenance (O&M) of several nuclear power plants (NPPs) in the United States has become financially burdensome to the point that the utilities may have to stop operation and retire their plants prior to the expiration of their operating license due to economic pressure. Moreover, the wholesale electricity prices have declined in some markets due to the increased penetration of renewables, such as wind and solar power, and the continued use of natural gas power. This phenomenon reduces NPPs' income from power generation. As a result, NPP operators aim to lower their O&M cost to ensure the plants can continue to produce electricity competitively.

The Department of Energy (DOE) has established the Light Water Reactor Sustainability (LWRS) program to assist NPP operators in sustaining their plant operations. The program has identified that the overall O&M cost to protect NPPs accounts for approximately 7% of the total cost of power generation, with labor accounting for half of this cost [1]. Within this overall labor cost, nearly 20% of it is needed to maintain the labor in physical security forces. The Nuclear Regulatory Commission's (NRC's) security requirements for commercial operating nuclear sites increased exponentially following the September 11th terrorist attacks resulting in a significant increase of onsite response force personnel across the nuclear industry [2]. The plant's response force includes the minimum number of armed responders, as required in the Title 10 of the *Code of Federal Regulations* (10 CFR) Part 73, and security officers tasked with assigned duties, such as stationary observation/surveillance posts, foot-patrol, roving vehicle patrols, compensatory posts, and other duties as required [3]. As labor costs continue to rise in the United States, any effort to reduce O&M costs needs to include a reduction in labor.

To support this mission, the LWRS program has established a pathway for physical security research. The physical security pathway aims to lower the cost of physical security through directed research into modeling and simulation, the application of advanced sensors, and the deployment of advanced weapons. These efforts are expected to reduce the NPP's active guard force for physical security. Modeling and simulation is used to evaluate the margin inherent in many security postures and evaluate alternative protective strategies to maintain overall security effectiveness while lowering costs [4]. By applying new technology, performing initial actions, or using additional plant safety equipment, many derived attack scenarios may no longer require specialized defense strategies and allow a reduction in the guard force. Detailed modeling and simulation of the reactor core and systems is necessary to evaluate whether these alternative protection strategies prevent core damage or provide more coping time for the reactor. This more inclusive process for physical security analysis is named Modeling and Analysis for Safety Security using Dynamic EMRALD (Event Modeling Risk Assessment using Linked Diagrams) Framework (MASS-DEF).

The LWRS research team has been working to apply the MASS-DEF methodology to operating NPPs in the United States [5]. In working with utilities to implement the MASS-DEF process, questions arose about whether the results of the different commercial physical security simulation tools used in the MASS-DEF process would be similar. Additionally, there were concerns about how differences in these results would impact the MASS-DEF process and the submission of security changes for regulatory review. The nuclear industry needs to pursue an optimized plant security posture that considers efficiencies and innovative technologies to help reduce costs while meeting security requirements. This report documents industry model comparisons between RhinoCorps' Simajin/Vanguard software and ARES Security's AVERT software for use in the MASS-DEF methodology.

2. OVERVIEW

There are four key functions in designing a physical protection system (PPS): deterrence, detection, delay, and response. The International Atomic Energy Agency (IAEA) outlines several phases in the design and evaluation of a PPS as shown in Figure 1 [6]. Evaluating the PPS and making changes to the PPS can be a very expensive process especially if done using drills, so many methods such as table-top exercises have been used to help reduce the drills needed. With modern computers, modeling simulation (MODSIM) tools capture most PPS factors and are now commonly used by PPSs for many different entities. A recent white paper prepared for NRC goes over guidelines for using MODSIM for physical security assessment [7].

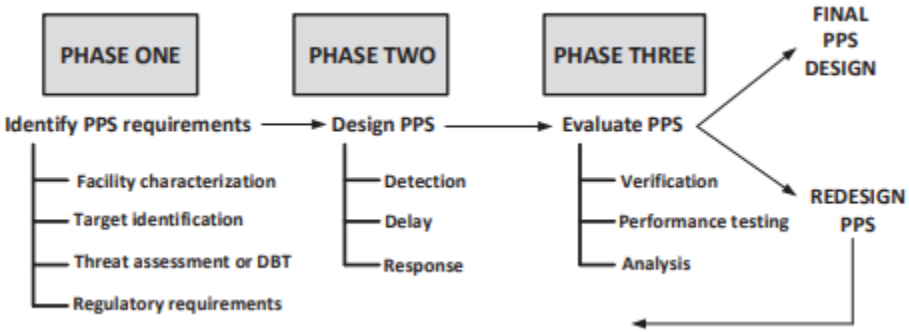

Figure 1. Phases for designing and evaluating a PPS.

2.1 Physical Security Simulation Tools

In our work with U.S. utilities, we have observed that commonly used tools include Simajin/Vanguard by RhinoCorps and AVERT by ARES Security. The AVERT software was developed in 1999 in coordination with the Defense and Threat Reduction Agency to protect U.S. nuclear assets. Their initial customer target was NPPs. Alternatively, Simajin/Vanguard was developed to provide advanced modeling and simulation solutions for various industries, including defense, security, and critical infrastructure protection. Their primary customer was initially the Department of Defense sites. Both have worked with NPPs to develop simulation models of their PPS and the software features to evaluate guard post positions, delay barriers, bullet resistant enclosures (BREs), or response strategies.

While each software tool has different algorithms and simulates scenarios differently, they have many of the same common principles and input criteria:

- Site Design – 3D models are used to make a plant layout matching detailed specifics of the actual site construction and terrain.
- Element Properties – Elements in the model, such as fences, walls, and doors, have properties that contribute to time factors, such as delay time and protection.
- Design Basis Threat (DBT) Development – This allows the user to specify attack agents, capabilities, resources, weaponry, etc.
- Target Sets – Specific targets can be added for attack scenarios with combinations of targets that constitute success.
- Detection – Various adversary actions can have a probability of detection associated with them which triggers the security protection strategy.

- Protection Strategy – The protection force is modeled along with defense strategies such as movement. Each guard has properties such as visual detection probability in a given range and hit-to-kill ratios.
- Scenario Development – Even though scenario development is different between Simajin/Vanguard and AVERT, each allows the user to specify features to represent different attack vectors that are determined by the physical security experts.
- Monte Carlo Simulation – Attack scenarios simulate the movement and strategies of adversaries and protection force using probability distributions with random sampling for events, such as shots hitting targets, delay times, etc.
- Results – Primary results consist of percent of runs where protection force prevents adversaries from taking out specified targets, used to calculate the probability of neutralization (PN) and the probability of effectiveness (PE). But other results include things such as kill ratios for guards, traversal times to targets, protection force losses, etc.

2.1.1 Simajin Features

Simajin/Vanguard's initial focus was DOE facilities and expanded to include nuclear facilities. Below is a list of features for Simajin/Vanguard, provided by RhinoCorps, showing what is most relevant to their security analysis customers:

- Fully autonomous combat simulation using an agent-based model running in large batches with a Monte Carlo simulation approach
- Based on a human model that provides a robust set of agents that can operate with only high-level instructions about tasks and objectives to perform their duties to accomplish a mission
- Human agents in the simulation have innate abilities that allow them to move in complex spaces, collaborate on tasks, dynamically use cover and concealment, operate vehicles in teams, use weapons and equipment, and communicate intelligence information
- High-fidelity representation of the breaching process that provides a realistic set of constraints for using mechanical and explosive breaches that require key resources in terms of personnel, tools, and methods
- Includes a simulation management tool that supports studies and analysis that allow large batches of simulations to be executed on a server farm and organizes results around study variables to help analysts evaluate conditions across different attack scenarios, defense strategies, facility designs, and other parametric inputs
- Includes a suite of reporting and analysis tools that allow for a detailed investigation of individual simulation runs as well as aggregate views of entire study cells with hundreds of runs to examine trends at a higher level.

2.1.2 AVERT Features

Although ARES Security's initial focus was the nuclear industry, they have expanded to other security areas. Below is a list of features in AVERT that they identify as offering additional value to their customers.

- Pathfinding: AVERT finds lowest-cost paths, where path cost can include any combination of time, exposure to detection, or exposure to firepower. This capability is used to generate attack plans for adversaries but is also used during a simulation to allow adversaries to dynamically replan and defenders to plan movements to intercept locations or defensive positions.

- Advanced behaviors: users can trigger behaviors based on dynamic conditions during simulation. Behaviors include using cover, small-team tactics like bounding overwatch, multi-stage breaching, and many others.
- Heat maps: users can visualize detection probability and firepower projection as a 3D overlay on their model.
- Simulation Controller: a web-based application that lets users run large numbers of simulations.
  - Multiple scenarios can be generated from a single base model.
  - A model hierarchy lets users maintain traceability on changes.
  - User management lets administrators define projects and assign projects to different users.
- Database reporting: The Simulation Controller has advanced result reporting options (e.g., contributions of defenders to neutralizations, adversary neutralizations by layer), and new reports are easily generated using SQL Server Reporting Services.

2.2 MASS-DEF Methodology

The MASS-DEF methodology consists of two parts: (1) the coupled modeling and simulation and (2) the post reduction process.

2.2.1 Coupled Modeling and Simulation

MASS-DEF incorporates simulations of attacks and factors in extra elements, like the timing of operator interventions and critical behaviors of safety systems, including the availability of pumps and the longevity of batteries. Dynamic modeling is adopted because the entire process of attack, response, operator actions, and plant responses is highly dynamic in that the timing and success or failures of one event affects the successes or failures of the next events. To correctly capture all these features, the dynamic modeling tool called EMRALD, which is also designed to couple with other simulation tools, was selected for this methodology.

EMRALD models the plant behavior and couples with a physical simulation tool and a thermal hydraulics tool as shown in Figure 2. The physical simulation tool provides the data specified in Section 2.1, to drive the plant behavior events in the EMRALD model. Finally, EMRALD modifies and executes a thermal hydraulics model with run specific timings to determine whether the adversaries successfully caused core damage.

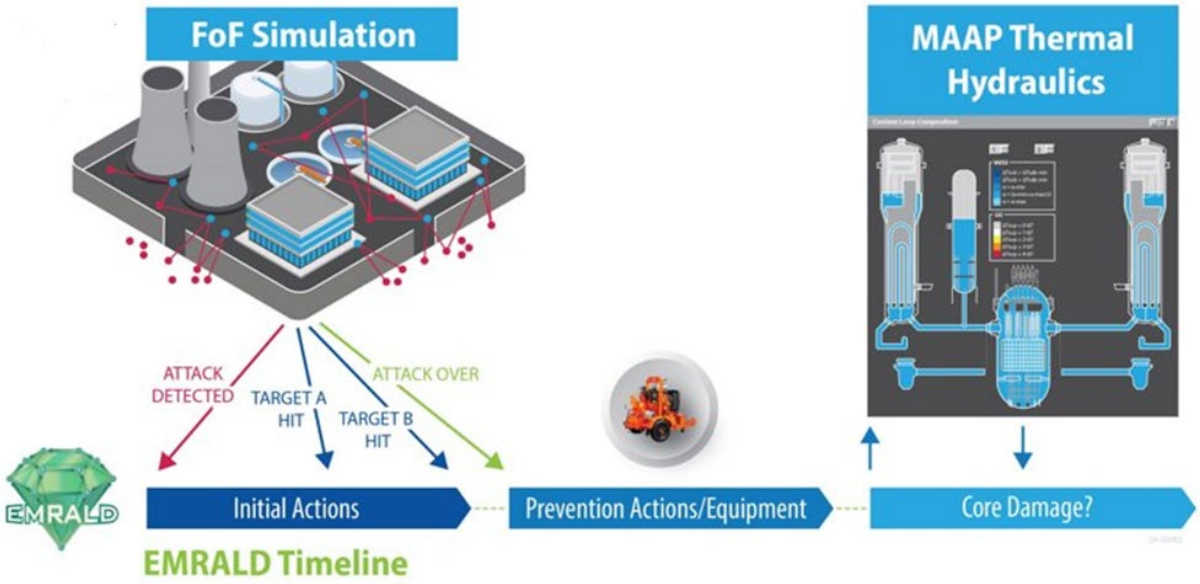

Figure 2. Coupling between the FoF simulation tool (Simajin/AVERT), EMRALD, and thermal hydraulics.

2.2.2 Post Reduction

The combined safety and security measures are modeled in an iterative process to refine the number of guard stations. Theoretically, by relaxing conservative requirements of PPS and by including preventive safety measures, a surplus of protective margin can be achieved. This extra margin is capitalized to remove the least effective guard station, using the outcomes of simulations as a guide, until the surplus is diminished to a level where the updated protection standard matches the original standard.

Figure 3 outlines MASS-DEF primary steps to refine the number of armed responders, and these steps are detailed below:

1. Analyze the baseline security simulation results to identify the least effective guard post throughout the scenario.
2. Exclude the identified least effective guard post from the security scenarios in the altered model.
3. Run the integrated safety-security simulation considering the defense alterations and removal of post(s).
4. Evaluate the results against the initial simulation results:
    a. If the conditional core damage probability (CCDP) is equal to or better than the original model results, recommence the process from Step 1.
    b. If the CCDP is inferior to the baseline model, then the security configuration from the previous iteration is kept and the process exits the reduction loop, proceeding to Step 5.
5. Implement the removal list on the initial potential strategy model. Execute and confirm that the outcomes are less effective than the original base case model.

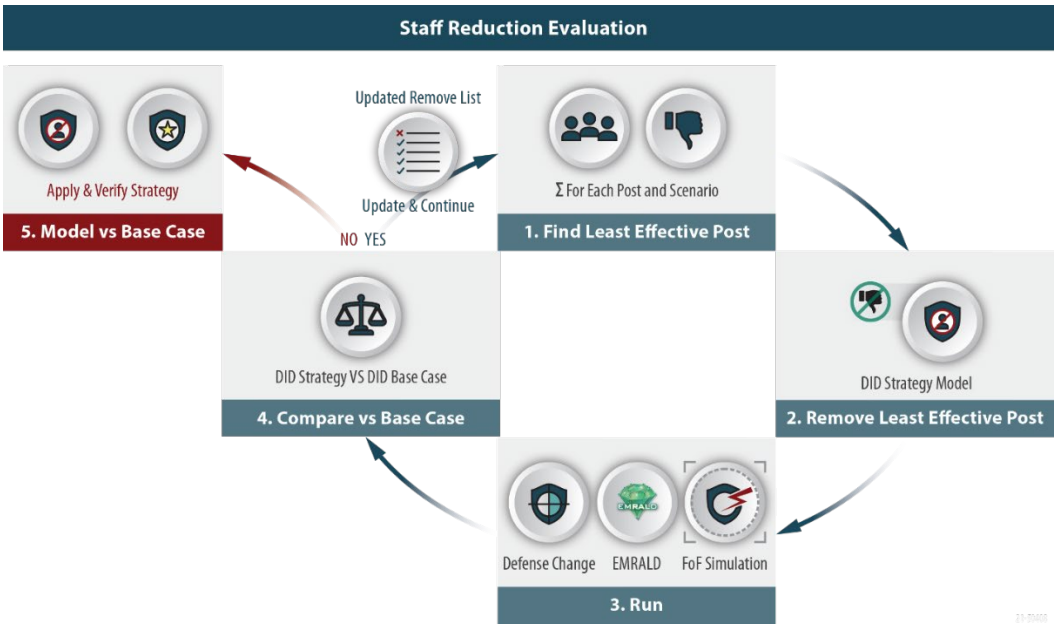

Figure 3. MASS-DEF general methodology.

Figure 4 shows a previous study on the application of MASS-DEF to a hypothetical nuclear plant8], where up to four guard posts were reduced without compromising the level of protection. However, note that these results may not be accurate because they do not reflect the complexities in actual NPPs. Therefore, the MASS-DEF application on actual plants is studied and discussed in the next section.

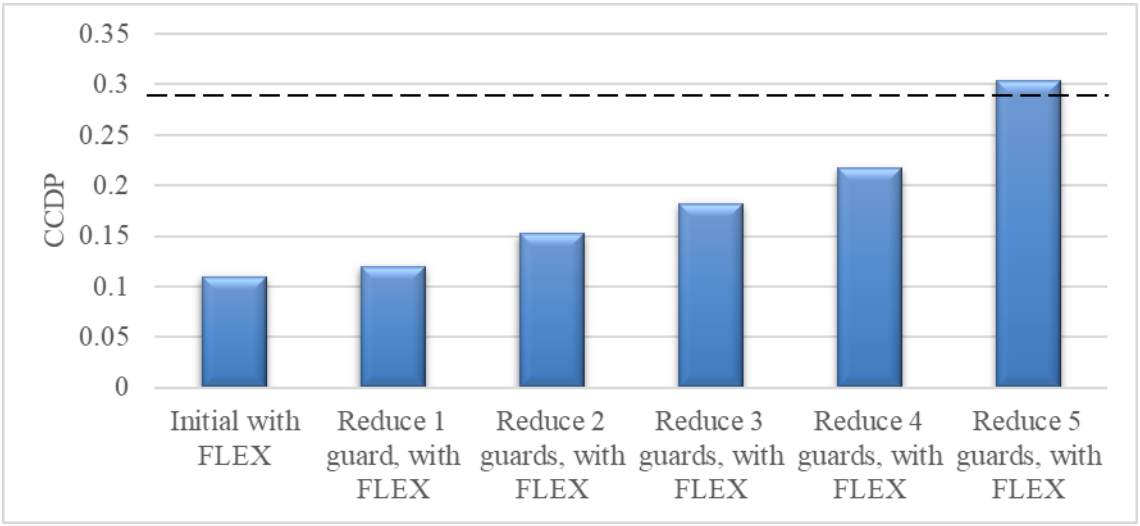

Figure 4. Guard post reduction process on a hypothetical nuclear plant [8].

2.3 Coupled Simulation Key Factors

While each model and tool runs mostly independently, there are a few timing features that are critical for each of the other tools. The physical security simulation runs first, and the results are read by the EMRALD simulation, then EMRALD sets up and executes the deterministic thermal hydraulics model for each run and waits for the result, which it reads to determine the final outcome, as shown in Figure 2. The following are the key timing points provided by or used by the simulation tools:

- Data sent from physical security simulation to EMRALD
  - Detection time (i.e., the time when adversaries are detected). This data is used for site defense strategies using operator actions, such as scramming the reactor, filling steam generators, deploying operators to specific locations, etc.
  - Target hit times (i.e., timings when targets in the nuclear plant are disabled by the adversary). These timing data affect the state of the plant and may be forwarded to the thermal hydraulic analysis tool. For example, the time when a cooling pump is sabotaged may determine a loss of coolant flow in the thermal hydraulic simulation.
  - Secondary target times (i.e., timings when secondary targets are sabotaged). Secondary targets include standby safety systems and components used in response to a sabotage attack to prevent unwanted safety consequences, such as an external pump connected to the FLEX (diverse and flexible mitigation capability) cooling connection.
  - Breach or entry times (i.e., the time or times when the adversary enters a specific area). This may be used to evaluate strategies with deploying operators to verify they can be safely executed.
  - Attack end (i.e., when it is believed that the guard force has neutralized the adversaries before complete target sets are hit or the adversary objectives are complete and the attack force is neutralized). This data is used to trigger the next stage in the scenarios, simulate after attack tasks, and complete the simulation of the plant response.
- Data provided by EMRALD to thermal hydraulics analysis tools
  - Trip time, which is the timing when the plant tripped from manual scram or from initiating event conditions.
  - Disabled equipment time, which is the timing when elements in the thermal hydraulics model are no longer available.
  - Equipment start time, which is the timing when elements in the thermal hydraulics model are to start up such as a manually operated cooling pump.
  - Simulation time, which informs how long to run the thermal hydraulics simulation before obtaining the results. Typically, a model would run for 8 hours, which is the standard reasonable assurance of protection time (RAPT) but can be adjusted according to specific sites calculations.
- Thermal hydraulics to EMRALD
  - Core damage time, which informs if and when the reactor core is damaged due to the attack scenario. This is used for final outcomes in EMRALD and for timing of statistical results.

3. COMPARISON STUDY

A utility agreed to collaborate with us on this research project. They had their existing scenarios modeled in AVERT. Additionally, RhinoCorps was performing some modeling at the same site for a different research project. This overlap provided a strategic opportunity for this comparison study. The existing AVERT results were shared by the utility and used along with the Simajin/Vanguard results to perform the comparisons. When the Simajin/Vanguard scenarios were created, it was assumed that they would be the same as those done for the AVERT analysis. However, the utility had made small changes to attack scenarios and defense strategies, which were used when creating the Simajin/Vanguard model. Therefore, adjustments had to be made, and the results rerun to complete the comparison.

Attack scenarios are evaluated as wins and losses; however, other data can be provided as well to determine post effectiveness or numbers for evaluating defense in depth. The win/loss data is a percentage of the percent, (wins)/(number of runs); this is used to calculate the PN, which is then used to calculate the PE. The win percentage part of the PN is what is being compared in this report.

3.1.1 AVERT Data Output

AVERT offers many options for running scenarios and then analyzing results or outputting data. This can be done through both the user interface (UI) (shown in Figure 5) and running from command line. Typical data output from AVERT consists of an attack plan summary, which shows each attack the win percent, shown as "P(e)", standard deviation for the win percent, shown as "StDev P(e)", and other numbers as shown in Figure 6. Data from each run including target and breach times is also output with an example shown in Figure 7.

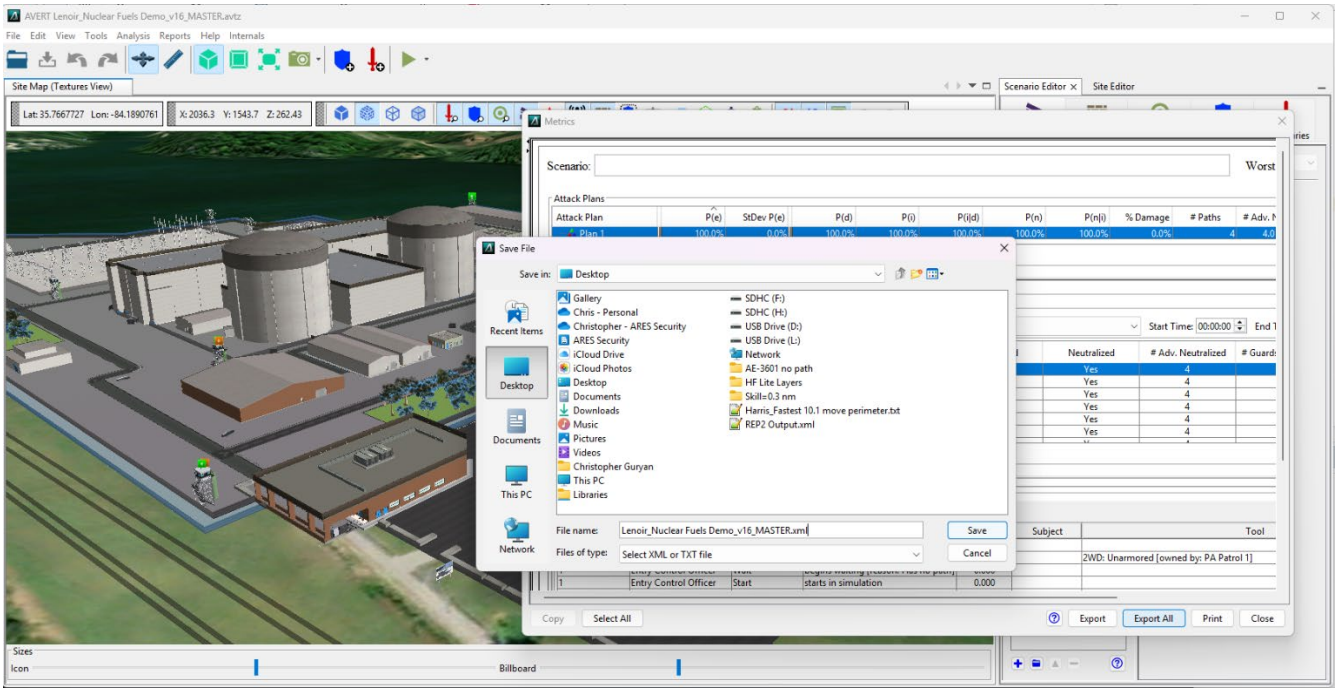

Figure 5. AVERT UI that allows the user to export results manually.

Plan	P(e)	StDev P(e)	P(d)	P(i)	P(i|d)	P(n)	P(n|i)	% Damage	# Paths	# Adv Neutralized	# Guards Neutralized	Traversal Time
Plan 1	0.91	0.029	1	1	1	1	1	0.33	3	4.87	4.98	443.638
Plan 2	0.88	0.032	1	1	1	1	1	0.333	3	4.82	5	463.084
Plan 3	0.91	0.029	1	1	1	1	1	0.312	3	4.9	4.78	431.828

Figure 6. Picture of tabulated results summary from AVERT in a spreadsheet.

Plan	Attack	System Effective	Detected	Interrupted	Neutralized	# Adv. Neutralized	# Guards Neutralized	Traversal Time
Plan 1	1	YES	TRUE	TRUE	TRUE	5	5	368.87
Plan 1	2	YES	TRUE	TRUE	TRUE	5	5	362.049
Plan 1	3	YES	TRUE	TRUE	TRUE	5	4	310.183
Plan 1	4	YES	TRUE	TRUE	TRUE	5	4	310.6
Plan 1	5	NO	TRUE	TRUE	TRUE	4	7	996.427

Figure 7. Picture of tabulated results for individual attacks in a spreadsheet.

A newer version of AVERT has a local web UI, which gives the user even more control of the data they can access and output and the type of files that are generated as shown in Figure 8.

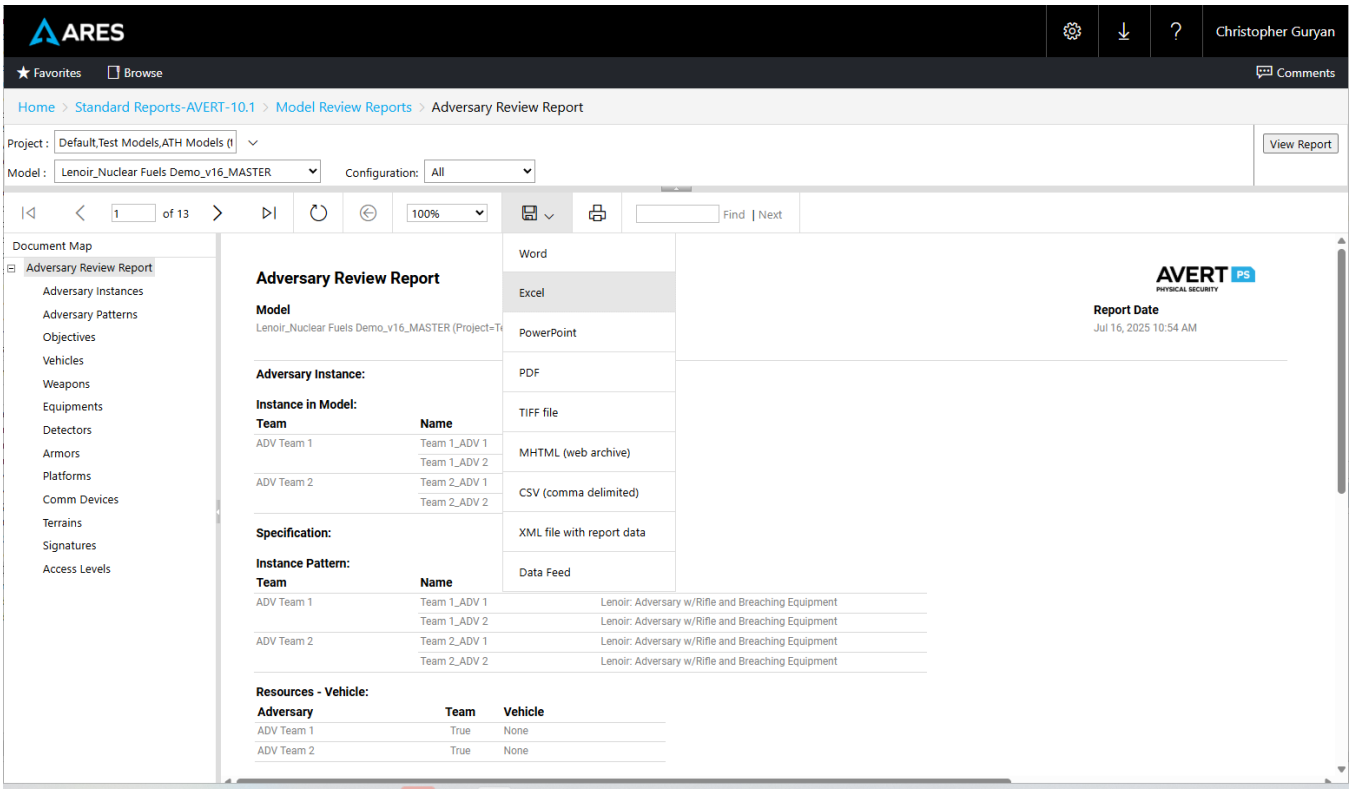

Figure 8. New AVERT web UI for more advanced data output.

3.1.2 Simajin Data Output

Simajin/Vanguard provides a rich set of reports and analysis tools that provide the user with a wealth of information that supports the evaluation of physical security system effectiveness and a comparison of alternatives. The simulation management interface is designed to support analysts with running, organizing, and analyzing large studies and can leverage large study farms to complete simulation batches quickly and effectively using available computing resources. Simajin/Vanguard includes a powerful 3D visualization tool that allows one to play back simulations and look at aggregate data sets to include movement paths and weapons fire as shown in Figure 9.

Simajin/Vanguard also allows for the export of results in an XML format. This allows for custom scripts or application to easily extract and process data using XML paths or other processing tools. Each run has a unique ID with the time or value for key parameters, such as detection time and breaches, as shown in Figure 10.

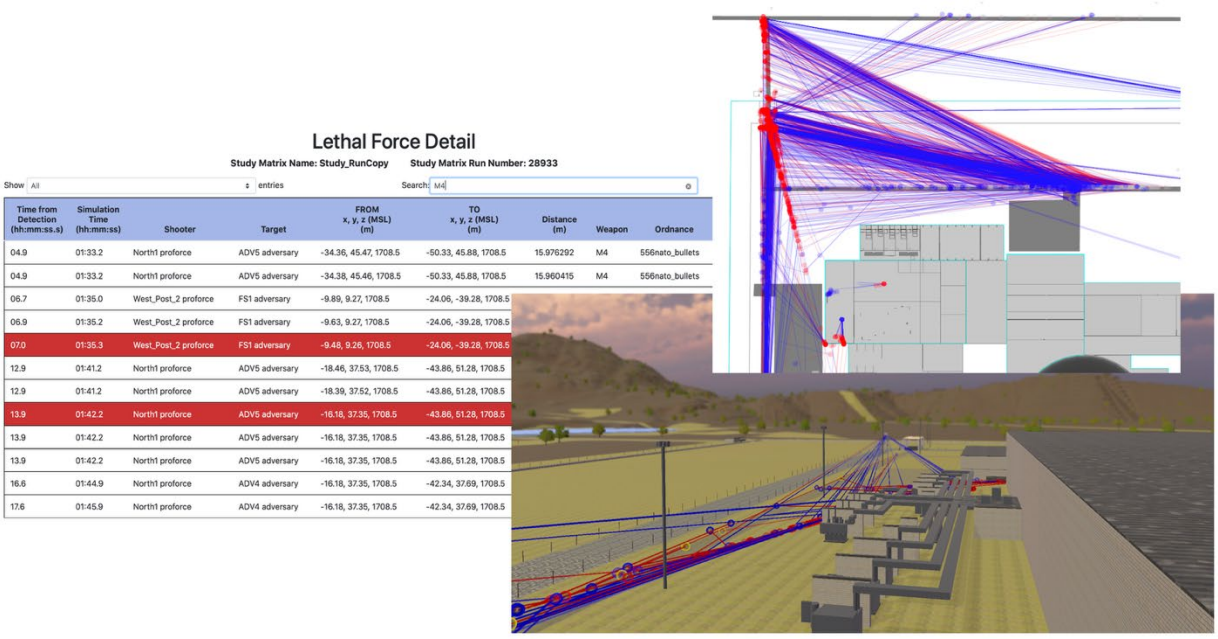

Figure 9. Examples of Simajin/Vanguard reporting products.

```
<study runs-per-cell="1" prefix="DID_FLEX_With_PF_07Nov2022_1Copy">
    <resultset date-executed="11/08/2022 11:46:11" result-id="215">
        <study-cell>
            <study-var name="Description" value="SC_1">
                <composite-var name="Graphics Configuration" value="NONE"/>
                <composite-var name="Protective Force Players" value="Normal_Ops_FLEX"/>
                <composite-var name="Facility" value="Facility_FLEX"/>
                <composite-var name="Attacking Players" value="SC_1_FLEX_DID"/>
                <composite-var name="End Simulation Early if Target Sabotaged" value="true"/>
                <composite-var name="Minimum Number of Protected Targets to Sabotage For a Win" value="2"/>
                <composite-var name="Simulation End Time (min)" value="30.0"/>
                <composite-var name="Sniper M110 Rounds per Salvo" value="1"/>
                <composite-var name="M4 PK Multiplier" value="0.75"/>
            </study-var>
            <run run-id="139224">
                <data name="ADV_deaths" value="8"/>
                <data name="ADV_kills" value="3"/>
                <data name="ADV_shots_taken" value="12"/>
                <data name="battle_time" value="167"/>
                <data name="first_detection" value="346.652954"/>
                <data name="first_response" value="354.747314"/>
                <data name="game-time" value="522.0"/>
                <data name="Inner_PA_breach_time" value="360.0401"/>
                <data name="MDP1_breach_time" value="473.072815"/>
                <data name="MDP2_breach_time" value="493.243591"/>
```

Figure 10. Picture of XML output from Simajin/Vanguard.

3.1.3 Comparison

Common statistical methods are used for comparisons. The first comparison looks at the win percentage for the utilities existing scenario analysis done with AVERT and the new analysis done with Simajin. As noted, these scenarios were not exactly the same, but many are very similar and have the same target sets. The intent of this first comparison is to show that a general comparison between the two shows similar win percentage results and if some scenarios do not then the causes can be analyzed and explained.

The run count and success count, where the guard force neutralized the adversaries, are put in adjacent rows where the win percent is calculated. The two sets of data are called a proportion comparison, and the "two-sample z-statistic" method was used to get a p-value. The "two-sample z-statistic" quantifies the difference relative to the variability, and the p-value helps in making a decision regarding the null hypothesis. In this case, the null hypothesis is that the PN value is the same for both test cases. A common significance level of 5% equates to a p-value of 0.05, so if the p-value is > 0.05, it is very likely that the hypothesis that PN values are equivalent is correct. Additionally, a confidence interval was calculated as a simple flag to indicate if the values are statistically equivalent.

The numbers for the actual calculations cannot be provided due to the sensitivity of the data, but an example of the setup is given below in Table 1. In Scenario 1, the high value shows that it is very likely that the scenarios are statistically equivalent. For Scenario 2, the p-value is very low, indicating that they are not very likely to be the same. Note that the "two-sample z-statistic" requires a large number of samples for a proportion comparison; we determined that around 500 samples provided reliable results indicated by low uncertainty in p-values, while at under 300 samples, we started to observe increasingly larger uncertainty in p-values.

Table 1. Example p-value calculation to compare the scenario results.

Scenario	Run Count	# Success		%		Pooled Proportion	z-statistic	p-value
1A	500	475		95%		0.945	0.693541982	0.487969489
1S	500	470		94%				
2A	500	475		95%		0.933	2.150159603	0.031542592
2S	500	458		92%				

For the AVERT-Simajin comparison, only the p-value and confidence intervals are provided and shown in Table 2. There was only one scenario (7) that did not fall within the confidence interval and had an p-value of <0.05. In this scenario, the targets were the same, but the defense strategy was altered, changing the win percentage significantly enough to affect the p-value and the confidence interval. Given the differences in the model, it is expected that there would be a difference for this scenario.

Table 2. Comparison results for several similar AVERT and Simajin scenarios.

Scenario	p-value	In Confidence Interval
1	1.0	Yes
2	1.0	Yes
3	0.28	Yes
4	1.0	Yes
5	0.16	Yes
6	1.0	Yes
7	0.014	No
8	1.0	Yes

Note that because of the high effectiveness of the plant defense strategies, only a few scenarios from the original AVERT scenarios resulted in adversaries achieving their target sets enough times to obtain statistical results for timing comparisons. For the MASS-DEF results to be useful, the timing of the events for target objectives need to be accurate or slightly conservative, conservatism and defense-in-depth modifications are made as part of developing an exaggerated model for the MASS-DEF process.

A more detailed comparison between the key event timings was done to verify that both tools provide statistically equivalent data for the same scenario. One scenario that had multiple delays, breaches, and targets was chosen for the comparison. This Simajin scenario was adjusted to match the strategy and paths of the adversary from the original results and was rerun for the comparison data. If the timing of the targets differed from the AVERT model, delays and breach times could be analyzed to determine the reasons for these differences.

A similar comparison method was used for the timing results; however, a T-Test function was used to get the p-value as there was timing data for each target and scenario. For each simulation run, the time for the different targets was added to a list in spreadsheet tab, and then, the standard deviation was calculated. A primary sheet collected the data from the different target and AVERT/Simajin runs and calculated the p-value along with the confidence interval. An example of these calculations is shown in Table 3 using test data. Table 3 shows us that the target timing data for both the first and second target are statistically equivalent, but the third target is not. Note that the T-Test function only requires a few samples compared to the z-statistic, which is needed in this situation because there are not very many results where the adversaries achieve their targets.

Table 3. Example calculations for target times between the two tools.

Spreadsheet	Sample Count	Mean Time	Std Deviation	Degrees of Freedom	Std. Error	p-value	In Confidence Interval
Target_1A	50	11.9	3.8926933	97.6377	0.8034	0.842554	Yes
Target_1S	50	12.06	4.1374842				
Target_2A	50	13.26	6.0434143	90.7306	1.0671	0.808044	Yes
Target_2S	50	13	4.5175395				
Target_3A	50	11.9	3.8926933	89.8072	0.93189	0.048969	No
Target_3S	50	13.76	5.3167429				

In the initial scenario RhinoCorp's modelers used their standard modeling practices for adversary attack behavior such as using cover, under fire delay, and blast standoff times. None of these initial results were within statistically acceptable ranges. It must be noted that this does not mean that one model is correct and the other not, it simply means that different strategies or modeling desires were being evaluated and compared. Given that the AVERT model was done several years earlier, it is unknown exactly why certain modeling features were used. Initial review of the models and results suggest that one model was significantly more conservative than the other. Several adjustments were made to the Simajin model to better match the AVERT model strategy. The final results for the target timing between AVERT and Simajin are given in Table 4, as with the other results data only the p-value and the confidence results are provided.

Only two early breaches matched between the two simulation result sets as shown in Table 4. As the simulations progress, the average times of the events grow further apart. This had a subsequent large impact on when the adversaries reached their objectives. The average time difference between the two tools for the target times was 49 sec. There was also a larger standard deviation in the times from one tool's target times vs the other, 15.6 vs 8.4 sec.

Table 4. AVERT vs. Simajin target timing comparison results.

Event	**p-value**	**In Confidence Interval**
Breach_1	0.60	Yes
Breach_2	0.00	No
Breach_3	0.99	Yes
Breach_4	0.00	No
…		
Target_1	0.00	No
Target_2	0.00	No
Target_3	0.00	No
Target_4	0.00	No

4. CONCLUSIONS

The MASS-DEF process uses event timings from physical security scenarios, such as detection, target completions, and assumed attack completion. This data can come from sampled statistics, if there is enough test data from security drills and FoF exercises to determine the statistics, or from physical security modeling and attack simulation tools. MODSIM tools enable the representation of more data sets for results, reducing uncertainty if the models are accurate and the tools implement correct methods. The more accurate the model and results, the more accurate the MASS-DEF outcomes will be.

Different MODSIM tools have different features that can affect the timing of attack scenarios such as manually assigning routes or automatic planning according to criteria such as using cover or fastest route. While there are values industry is to use for things like Hit-to-Kill ratios and run speeds, there is currently no standard of practice to determine what options should be used for many other MODSIM capabilities. Physical security experts currently use the tools to help evaluate many different attack and defense options with the goal of protecting against the most effective and probable attack scenarios. The comparison results of this report show that in general, expert modeled scenarios have similar outcomes, suggesting there is no significant outcome differences between using the tools. However, specific events and timing features can be significantly different and could impact outcomes if these timings are used in the MASS-DEF or similar processes. Overly conservative factors in a model can be used to help evaluate defense-in-depth features or perform specific "what if" cases, but if target timing is used for MASS-DEF then it is recommended that the data and modeling features be as close to realistic as possible. Especially since when performing post reduction evaluation, an exaggerated model is used to calculate post engagement. Having compounding conservatisms would cause significant negative impacts to the strategy evaluations. A standardized process for both developing and reviewing PPS similar to what is outlined in [7] would be extremely beneficial for the MASS-DEF process and also highly valuable for new advanced reactor site evaluations. It is recommended that before using a MODSIM model with MASS-DEF that it be reviewed against a standard of practice to make sure it will be as effective as designed and over conservatisms or inconsistencies don't cause large impacts on the strategy change evaluation results.

5. REFERENCES

1. PG&E. 2018. "PG&E Company 2018 Nuclear Decommissioning Cost Triennial Proceeding Prepared Testimony – Volume 1." 18-12 (U 39 E), Pacific Gas and Electric Company. https://analysis.nuclearenergyinsider.com/pge-seeks-decommissioning-head-start-cost-estimates-rise.
2. U.S. NRC. 2020. "Emergency Preparedness in Response to Terrorism." About Emergency Preparedness, U.S. Nuclear Regulatory Commission. Last modified Nov. 13, 2020. https://www.nrc.gov/about-nrc/emerg-preparedness/about-emerg-preparedness/response-terrorism.html#one.
3. U.S. NRC. 2021. "PART 73—Physical Protection of Plants and Materials." (NRC, 10 CFR), U.S. Nuclear Regulatory Commission. Last modified Mar. 24, 2021. https://www.nrc.gov/reading-rm/doc-collections/cfr/part073.
4. NEI. 2016. "Diverse and Flexible Coping Strategies (FLEX) Implementation Guide." NEI 12-06, Rev. 4, Nuclear Energy Institute. https://www.nrc.gov/docs/ML1635/ML16354B421.pdf.
5. R. Christian, S. R. Prescott, V. Yadav, S. St. Germain, C. P. Chwasz. 2022. "Evaluation of Physical Security Risk for Potential Implementation of FLEX using Dynamic Simulation Methods." INL/RPT 22 70315, Rev. 0, Idaho National Laboratory, Idaho Falls, ID. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_64424.pdf.

6. IAEA. 2021. “Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities.” IAEA Nuclear Security Series No. 40-T. https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1875_web.pdf.
7. Talbot, Matther, Dan Corquidale, and Jim Anderson. 2025. “Guidelines for Implementing Physical Security Assessments using Modeling and Simulation in the Nuclear Industry.” https://www.rhinocorps.com/rhinocorps-guidance-documents/
8. R. Christian, V. Yadav, S. R. Prescott, and S. W. St. Germain. 2022. “A Dynamic Risk Framework for the Physical Security of Nuclear Power Plants.” Nuclear Science and Engineering 197, no. 1 (2022): pp. S24 S44. https://doi.org/10.1080/00295639.2022.2112899.