Using Fully Automated Combat Simulation to Support Security by Design

Dan McCorquodale, Matthew Talbot
RhinoCorps Ltd. Co, Albuquerque, NM

Abstract

Modeling and simulation tools are used extensively to support design and operational decisions at nuclear facilities across many domains. RhinoCorps provides support for vulnerability assessments using a fully automated combat simulation primarily at these types of facilities. The robust human model that is the core part of the Simajin/Vanguard software provides a set of innate abilities that allows analysts to rapidly model attack scenarios, defense strategies, and define highly detailed three-dimensional models of facilities and terrain. Using a Monte Carlo simulation approach analysts can explore a wide range of outcomes to evaluate the effectiveness of a physical protection system for nuclear or other high value facilities. This software has been used extensively for the last fifteen years to support vulnerability assessments at dozens of government sites and commercial sites throughout the United States and internationally.

The use of Simajin/Vanguard has supported "Security by Design" for multiple organizations helping to inform construction requirements, defensive features, force size and composition, and other elements that support the physical protection system prior to construction of the facility. Although most of this support was for expansion/transition of government facilities it has also been employed in the commercial sector for at least one small modular reactor. This approach has provided large savings in time and money by incorporating a security mindset early in the design and construction process. This paper provides a roadmap for applying combat modeling and simulation tools for new plant designers as well as existing plants considering major changes in their facility. The roadmap identifies key challenges likely to be encountered when a real plant with a real protective force does not exist, as well as an approach to overcoming those challenges. The roadmap and underlying processes are iterative and support an evaluation of security during conceptual design, detailed design, construction, and operational phases of the facility. Included in the process are strong fundamental approaches to accreditation as each iterative step occurs, which is particularly important as many key performance measurements will be unavailable in the early stages.

Keywords: Modeling and Simulation, Combat Simulation, Simajin, Vanguard, Security by Design

Introduction

The reduction of the overall operational cost for nuclear power plants is important to maintaining the viability of nuclear energy as a carbon-free and competitive source of energy in the U.S. and throughout the world. Physical security is one of the primary drivers for operational cost and it does not increase revenue nor productivity of the plant. According to the Light Water Reactor Sustainability program security represents 7-12% of the total operational cost to produce electricity.[1]

Existing power plants are limited by their existing designs and inherent vulnerabilities/targets, and as such may have less opportunity to reduce security costs because of the constraints of working at an operating plant and the high capital costs associated with retrofitting security elements into the design. However, advanced reactors and new builds of existing reactor designs have an opportunity to implement security by design, and high-fidelity combat simulation offers a capability to objectively evaluate physical security system designs, even in the absence of an existing physical site.

Methodology

With security by design, security managers and designers will have the tools and results to influence or even require certain construction materials as well as control how people can move within the facility. These choices can drive the adversary to select routes or breach certain obstacles that are advantageous to the security forces. This in turn allows for optimal placement of security features like defensive fighting positions or detection systems. Unless the targets themselves can be removed from the equation, there is likely to be some form of on/off site response and in particular any off-site support will have to rely on both early detection and substantial delays; this will be made possible by decreasing vulnerabilities at the physical design level for new advanced reactors and new builds of traditional designs.

One key problem in incorporating security by design for a new build is that there is no real-world site to evaluate, and there are no security officers and physical protection system (PPS) that can be performance tested at that non-existent site. However, there are still proven tools that can help address this issue. Automated combat simulation can support evaluation of numerous plant designs along with the security systems and strategies. While an existing site has the benefit of being able to collect performance data and conduct limited scope performance testing as well as full scale exercises; using simulation to support security by design for a site that has not been built yet requires leveraging industry-based performance data. When new and advanced technologies are being considered, vendor supplied performance data along with subject matter expert judgement provide a sound basis to start the process. If there exists large discrepancies or gaps in performance data, sensitivity studies can be conducted to help identify minimum acceptable performance characteristics that will yield acceptable risk values. As more independent performance data is collected for new technologies the models used for this type of analysis can be updated.

This means that cost-benefit analysis can be conducted on various security strategies for a given power plant design and this can happen before construction starts and thus can influence many aspects of that power plant design.

Automated Combat Simulation

RhinoCorps' Simajin/Vanguard is a fully automated combat simulation, and for the purpose of this presentation will be used to illustrate how combat simulation can support security by design. Simajin is the three-dimensional (3D) simulation engine that is used to represent the facility, the defensive strategy, and various user-defined attack scenarios. Simajin has a legacy supporting military systems and conflict. It is a general-purpose agent-based modeling and simulation engine that facilitates Monte Carlo style analysis by running thousands of simulations. Vanguard is the data that supports modeling physical security in urban and industrial environments, and it defines the people, weapons, facility features, vehicles, equipment, explosives, detection systems, and the other things needed to conduct vulnerability assessments at nuclear and other high-security facilities.

Simajin/Vanguard has been used within the Department of Energy (DOE) for more than 15 years and supports Nuclear Regulatory Commission (NRC) licensee sites in the US as well as international sites. Simajin/Vanguard has also been used to support analysis of security strategies for advanced reactor designs. Simajin/Vanguard is an accredited and proven tool that provides an objective evaluation of physical security, which is an important consideration when doing an analysis for a pre-construction facility.

The Process

The process described in this paper is based upon real-world applications of Simajin/Vanguard used to support security by design for over ten years. This prior work has helped balance facility designs within the DOE and for advanced reactors to yield more cost-effective implementations that are highly secure. This process is executed by a team of specialists that can support the design process and the analysis of the various security designs being considered.

Before the analysis process begins there are prerequisite activities that should be completed. As the security by design process is iterative many of the prerequisites can mature throughout the cycles of analysis in tandem. At a minimum there needs to a conceptual layout of the plant with its major components, and there needs to be an initial target set analysis to identify vital equipment along with methods of damaging or compromising the target set elements. In early stages of analysis, assumptions can be made that facilitate early analysis without fully understanding the target set requirements for sabotage.

There also needs to be a concept for the physical protection system and the defensive strategy that supports that system. The concept for the PPS will evolve as the analysis proceeds, but there should be a set of working assumptions about which technologies might be employed and how the response force will be expected to protect the plant. Country specific regulations will define many requirements that must be addressed and provide a foundation for security personnel and their functions, detection systems, access control systems, and other operational elements of the plant.

The analysis team will need to have a strong foundation in the regulatory requirements as well as knowledge and experience working with security systems, weapons, and tactical response. The design basis threat (DBT) defined by the regulatory body is a key element in supporting the analysis process as it defines adversary capabilities which will be used to measure the success or failure of the PPS.

Without the key items described above it is too early to begin using combat simulation. These items can and should evolve through the iterative cycles in the process, but there needs to be enough detail to define a conceptual facility model, defense strategy, and some DBT compliant attack scenarios before there is any value in initiating the process of analyzing the PPS with combat simulation. The pages that follow elaborate on the analytical process used to apply combat simulation in security by design. Figure 1 below provides an overview of the steps in this iterative process.

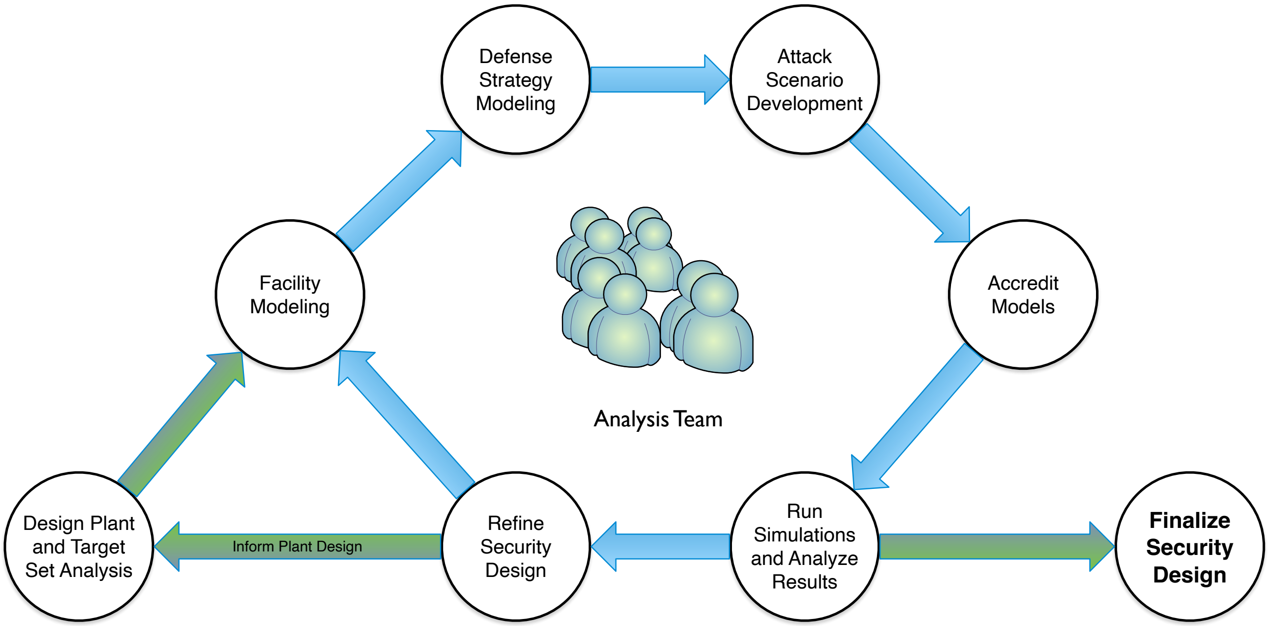

Defense Strategy Modeling
Attack Scenario Development
Facility Modeling
Accredit Models
Analysis Team
Design Plant and Target Set Analysis
Inform Plant Design
Refine Security Design
Run Simulations and Analyze Results
Finalize Security Design

Figure 1 – Iterative Process to Apply Combat Simulation to Security by Design

Facility Modeling

When employing security by design as a process with a pre-construction project it is most cost effective to engage as early as possible and expect to iterate the security strategy as the design of the plant itself proceeds. In today's world we expect that plant designs will be predominantly performed using computer aided design (CAD) tools and that a 3D model will exist for the key buildings. These 3D models can be used to create the corresponding facility model in the combat simulation thus providing a quicker path to evaluating security concepts. Perhaps some representation of the protected area and other exterior features will also exist. Depending upon the type of project there may not be a specific site identified for the plant, such as for an advanced reactor design that is undergoing design certification as opposed to an application for an operating license.

Regardless the data that does exist for the main buildings and other supporting elements (e.g., barriers, supporting structures, etc.) can be used to build a facility model for the combat simulation. The CAD drawings can be imported and converted to conform to a Simajin/Vanguard specific facility model. Generally, the CAD drawings will not contain all of elements of the PPS so these features will need to be included to represent things like detection systems, cameras, barriers, and defensive fighting positions. If needed, a notional terrain can be used to locate the facility model at some point in space. Some consideration should be given to the expected types of locations that the hypothetical plant could be placed. For advanced reactors or small modular reactors, the long-range plan will likely be to build numerous installations of the plant. The expected installations may be in remote areas or in urban areas, and understanding the types of locations will have an impact on which notional terrain data might be used. This knowledge will also influence decisions about the defense strategy.

The benefits of creating a facility model in the combat simulation will be immediate. This by itself provides a useful capability for security planners to visualize the site and even conduct simulation-based tabletop exercises to explore ideas and concepts. Tabletop exercises will feed into the subsequent phases of this process as the defense strategy and attack scenarios are developed and refined.

Security planners can propose and model variations of the facility layout to include specifying security layers with their corresponding barriers and intrusion detection systems. This stage provides a useful way to explore employing new technologies, to define protected areas that optimize spacing to afford ample engagement opportunity, or other aspects of the PPS that will reduce cost and enhance security.

Defense Strategy

With a facility model and potential variations in place security planners can begin to consider and evaluate different strategies. At this stage new technologies and novel approaches to securing the facility can be modeled. This informs the strategy and variations to affect the intrusion detection systems, situational awareness systems, engagement positions, and other mechanisms for controlling or encouraging adversary paths.

While at an early stage in the design process one can make considerations that balance security operations with plant operations. For example, are there ways to reduce when and who can go into the protected area? Can we limit vehicle entries into the protected area? Both of those factors determine how many security officers are needed to do searches and control entry. Can technology be used to reduce personnel requirements in support of entry and exit from the protected area?

These strategy alternatives can now be modeled in anticipation of evaluating each of these with the combat simulation tool. Note, proposed security strategies can have implications on the facility model, so be prepared to update or generate the corresponding facility models in support of the upcoming analysis. As iterations in the analysis process proceed some alternatives may be dropped and new ones postulated.

As an integral part of placing defensive fighting positions; remotely operated weapon systems; ballistic and bullet resistant enclosures, cameras; and other detection systems within the facility the modeling tools should be used to develop coverage maps to ensure that no blind spots exist that would provide an advantage for the adversary as they attempt to traverse the facility and reach target set elements. The sensor and weapon coverage maps can also be used to ensure that the facility has space to support clear engagements of potential adversaries moving to the vital areas of the facility.

Attack Scenario Development

With a set of candidate defense strategies developed the process of defining attack scenarios can be initiated. Depending upon the maturity of the defense strategy and/or the facility model, analysts can establish adversary success criteria that are practical and sufficient. As an example, during early stages of the security design process or based upon the nature of the strategy the adversary scenarios can be considered successful simply by arriving at key areas of the facility such as gaining access to the reactor building. This can simplify the early stages of analysis such that the security planners can more quickly iterate through alternatives of the defense strategy. This analysis strategy also allows the security assessments to be somewhat decoupled from the detailed design of building interiors during early stages where frequent design changes are to be expected.

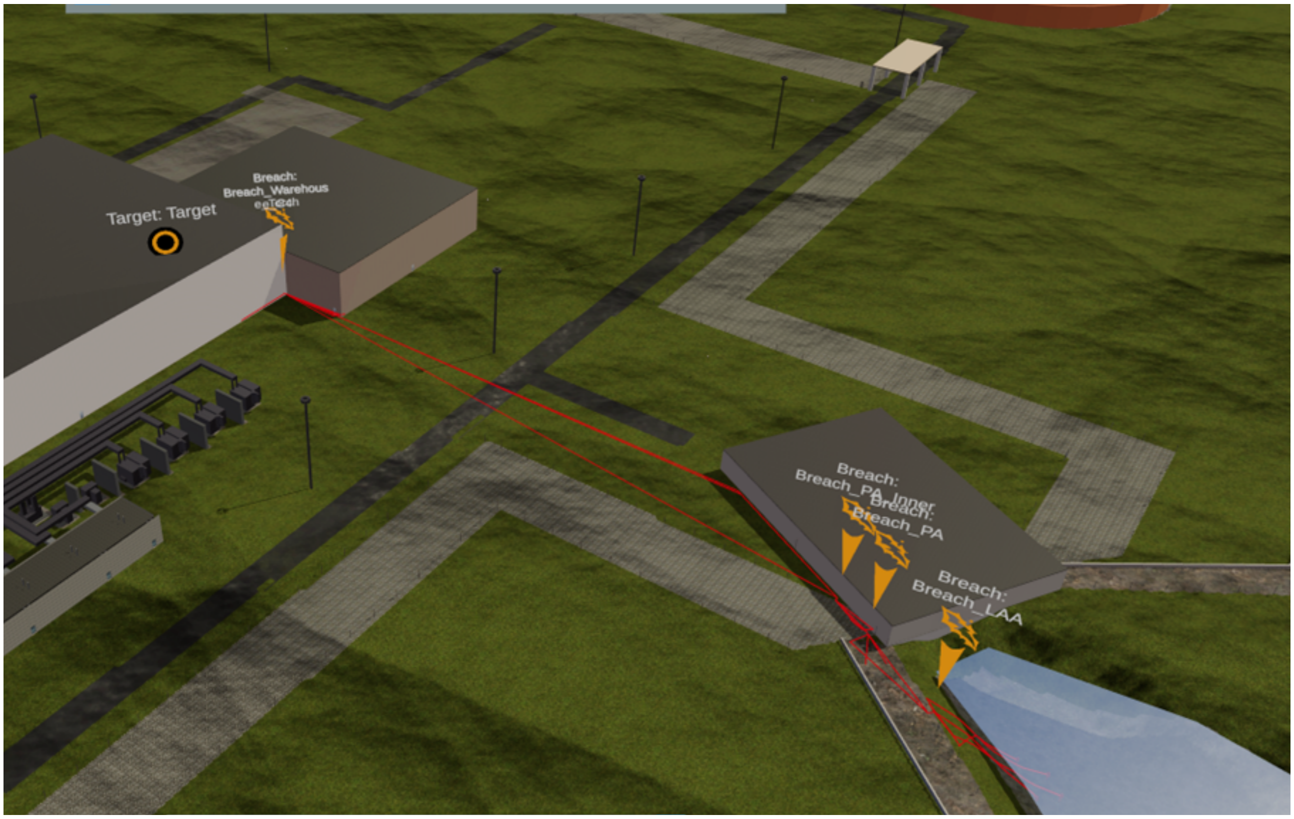


Figure 2 – Attack Plan Example

Using the facility and defense strategies the analysis team can develop attack scenarios using subject matter expertise and/or pathway analysis. Pathway analysis is an automated technique for identifying potentially advantageous avenues for the adversary to use when attacking the facility. A pathway analysis will generally have to make assumptions about response, delay, and detection parameters to identify notionally desirable routes for an adversary; it will not however touch the combat/engagement aspects that yield “how successful” the route might be for an adversary. When using pathway analysis to develop concepts for scenarios it is important to recognize that subject matter experts will still be needed to produce the additional details required to make that conceptual scenario into something of real-world quality. Supporting elements of the attack force, diversionary tactics, and tactical approaches are important to include in the attack scenarios and are the things that make a scenario representative of what a capable and prepared adversary will do. Pathway analysis falls short of specifying these important elements, because it is still a very challenging computational problem that brute force cannot overcome with sufficient quality.

The scenario development process should strive to specify attacks that stress the defense and exploit perceived weaknesses as much as possible. This includes coming from different directions and addressing all engagement elements. One should note that specific attack variations may be required that correspond to specific defense or facility model variations. This process of attacking from a variety of vectors will allow the operator to understand the value, in totality, of each defensive element.

When starting the scenario development process, it is important to start with straightforward attack plans that can be quickly employed to exercise the defense of the facility. As iterations in the process proceed the attack plans will be refined to stress the defense in a broader range of directions and methods of attack. The final analysis should include many scenarios that use different techniques for defeating barriers, attacking the defensive personnel and weapon systems, and reaching the target set elements. Evaluating this large set of scenarios against the defense alternatives will provide high assurance in the design of the PPS.

Running Analyses

With conceptual/candidate facility models, defense strategies, and attack scenarios in hand the combat simulation can now be leveraged to evaluate the effectiveness of the defense strategies. This stage of the process will require several iterations and will follow a rigorous model accreditation process. Once the models are accredited, the simulation will be executed hundreds of times for each combination of strategy, facility, and scenario producing results that can be used directly to rank the performance of the strategies and provide insights into why or how the strategy failed or succeeded.

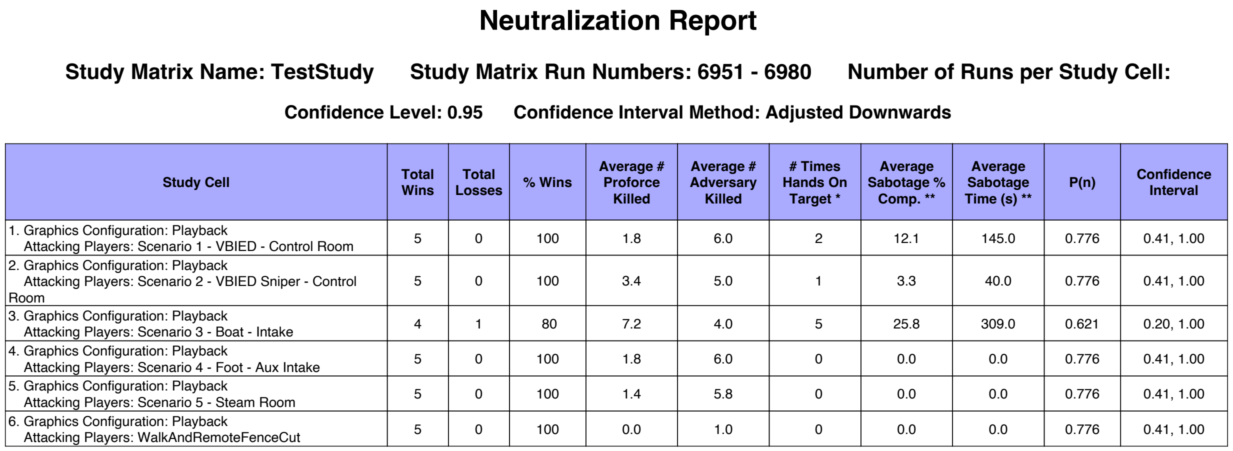
Unlike for operational facilities, at this phase in the security by design process there typically is no basis for performance testing that is needed to establish high-confidence response times, alarm dispatch times, probabilities of detection, and other important figures of merit that feed into the simulation. As appropriate, industry exemplars for performance or subject matter expertise should be used to provide those initial estimates of performance. Additionally, the use of uncertainty analysis can play an important role in the simulations. The analysis tools easily allow for use of random distributions for inputs into the simulation that realistically represent the range of performance for adversary and protective forces. This can affect breach times, breach success, sabotage times, response times, dispatch times, and operator actions. Using these distributions, the simulation results will produce a broader range of outcomes, which will help identify potential vulnerabilities to address or strengths that can be leveraged.

As indicated earlier in Figure 1, this process will be iterative and for each iteration the security planners will learn about how the security design works and how it doesn’t. The process will revisit the facility model, defense strategies, and attack scenarios to continue the refinement process. It is likely and expected that the plant design itself may pose issues for the security effectiveness. It is possible that changing construction materials, placement of laydown yards or other clutter, placement of protected area barriers, or other elements of the plant design can greatly impact security system effectiveness.

The ability for security planners to affect aspects of the plant design will vary by organization. This will be an important consideration for how the defense strategy evolves. Both capital costs for the construction of the plant and its security systems contrasted with the expected operational and maintenance costs for the security personnel and systems will factor into the cost-benefit analysis. It may not be practical to expect making the exterior walls three meters thick just to force the adversary through a few key entrances. This will be part of the balancing act that ultimately leads to the best security design that is also practical.

Evaluating Alternatives

Once there are sets of simulation runs for a suite of alternatives, analysts can directly compare the benefits and cost of one configuration to another. Probability of system effectiveness (P_E) is the top-level measurement for how well the PPS performs and provides a quantitative risk assessment value.[2] P_E is computed using probability of interruption (P_I) times probability of neutralization (P_N). Probability of interruption for a given set of designs is generally high (when onsite defenses are present or there are substantial delay times) and is also relatively consistent, so the larger factor in success tends to be probability of neutralization, which is a conservative statistically based measure of the percentage of wins by the defensive side. Often one can start by comparing the percentage of wins between the various alternatives. A report like the Neutralization Summary, provided in Figure 3, provides an easy way to see data like this along with the statistical confidence levels for each scenario.



Neutralization Report

Study Matrix Name: TestStudy   Study Matrix Run Numbers: 6951 - 6980   Number of Runs per Study Cell:

Confidence Level: 0.95   Confidence Interval Method: Adjusted Downwards

Study Cell	Total Wins	Total Losses	% Wins	Average # Proforce Killed	Average # Adversary Killed	# Times Hands On Target *	Average Sabotage % Comp. **	Average Sabotage Time (s) **	P(n)	Confidence Interval
1. Graphics Configuration: Playback Attacking Players: Scenario 1 - VBIED - Control Room	5	0	100	1.8	6.0	2	12.1	145.0	0.776	0.41, 1.00
2. Graphics Configuration: Playback Attacking Players: Scenario 2 - VBIED Sniper - Control Room	5	0	100	3.4	5.0	1	3.3	40.0	0.776	0.41, 1.00
3. Graphics Configuration: Playback Attacking Players: Scenario 3 - Boat - Intake	4	1	80	7.2	4.0	5	25.8	309.0	0.621	0.20, 1.00
4. Graphics Configuration: Playback Attacking Players: Scenario 4 - Foot - Aux Intake	5	0	100	1.8	6.0	0	0.0	0.0	0.776	0.41, 1.00
5. Graphics Configuration: Playback Attacking Players: Scenario 5 - Steam Room	5	0	100	1.4	5.8	0	0.0	0.0	0.776	0.41, 1.00
6. Graphics Configuration: Playback Attacking Players: WalkAndRemoteFenceCut	5	0	100	0.0	1.0	0	0.0	0.0	0.776	0.41, 1.00

Figure 3 – Example Neutralization Summary Report

There will be cases in which the P_N values between two alternatives are statistically insignificant, so to further understand how well those alternatives match up against each other one can use security layer statistics reported by the simulation. These layer statistics can identify how many adversaries made it into the vital area on average between the alternatives. Time may also be an important factor for success in that plant operations may be able to take actions to put the plant into a safe mode if given ample time to react, so part of the defense strategy can include delaying the adversary from reaching vital equipment so that plant operations can take those critical actions. In this situation using the timing values for breaches and layer penetration provided by the simulation output can also help in the evaluation process.

Conclusion

The results of the overall process will also be valuable beyond the design phase and can directly support the licensing process as well as the ongoing training and vulnerability analysis that comes with operating the actual plant.

"Security by Design" can be accomplished using combat simulations to qualify a site's security system effectiveness which will help inform construction requirements, defensive features, force size and composition, and other elements prior to construction of the facility. In many cases, plant design decisions that negatively impact security, and thus the cost to operate the site, are simply due to the absence of quantitative security analysis that could have informed the facility design. Tools and processes are available and, in some cases, have already led to lower operating costs as well as a cohesive security strategy.

Plant designers and operators should strive to quantify potential security strategy alternatives early and often in the design of the plant and site. Costs to perform this iterative analysis are a fraction of the savings generated from simply saving a single post, and identifying potential vulnerabilities earlier in the design and construction phase can save significantly more money. Depending upon the level of detail and complexity of the facility design and how broadly one considers alternative defense strategies using combat simulation is relatively inexpensive. Typically, the elimination of a single post can recoup the expense of using combat simulation within one or two years.

References

[1] Light Water Reactor Sustainability Program, "*Integration of FLEX Equipment and Operator Actions in Plant Force-On-Force Models with Dynamic Risk Assessment*", August 2020, U.S. Dept of Energy, Office of Nuclear Energy

[2] Talbot, Matthew and McCorquodale, Dan and Broglie, Ian "*Computing Physical Security System Effectiveness at Commercial Reactors.*" Nuclear Science and Engineering, 2022 Month 10, doi: 10.1080/00295639.2022.2120315