Dynamic Risk Framework for Optimizing the Physical Security Postures of Nuclear Power Plants

Robby Christian[a], Vaibhav Yadav[b], Steven R. Prescott[c], and Shawn W. St. Germain[d]

[a] Idaho National Laboratory, Idaho Falls, USA, Robby.Christian@inl.gov
[b] Idaho National Laboratory, Idaho Falls, USA, Vaibhav.Yadav@inl.gov
[c] Idaho National Laboratory, Idaho Falls, USA, Steven.Prescott@inl.gov
[d] Idaho National Laboratory, Idaho Falls, USA, Shawn.StGermain@inl.gov

Abstract: This paper describes an ongoing effort within the Light Water Reactor Sustainability program at Idaho National Laboratory to optimize the security and costs of nuclear power plants (NPPs). It introduces Event Modeling Risk Assessment Using Linked Diagrams (EMRALD), a dynamic risk assessment tool developed at Idaho National Laboratory. EMRALD was leveraged to optimize NPP security postures by integrating force-on-force (FOF) simulations and operator mitigation actions, including dynamic and flexible coping strategies (FLEX).

To illustrate the methodology, four attack scenarios were modeled via a commercially available FOF simulation tool, using a hypothetical NPP facility. The simulation results provided valuable insights into possible attack outcomes, as well as the probabilistic risk of core damage events given these outcomes. Safety mitigation procedures dependent on the attack outcomes were modeled in EMRALD by considering human operator uncertainties.

The results demonstrate that the number of armed responders can be optimized while still affording the same level of protection as in the initial security posture. The proposed modeling and simulation framework created by integrating FLEX equipment with FOF models enables NPPs to credit portable FLEX equipment in their security postures, resulting in an efficient and optimized physical security system.

1. INTRODUCTION

Increased penetration of natural gas into the deregulated energy market in the U.S. has created financial challenges for baseload power plants such as nuclear power plants (NPPs). Because of the nuclear materials employed, NPPs are saddled with an additional cost burden in protecting fuel against sabotage. The overall operational and maintenance costs of such protection account for approximately 7% of the total power generation costs, with labor accounting for half of that 7% [1]. In the current research, interaction with utilities and other stakeholders led to the determination that physical security forces account for nearly 20% of the entire workforce at several NPPs.

The Department of Energy established the Light Water Reactor Sustainability (LWRS) program to support the current fleet of NPPs by producing research that fosters reductions in operational and maintenance costs. This paper describes a methodology proposed within the LWRS program to optimize NPP security postures in regard to protection levels and operator mitigation responses workforce, in continuation of our previous paper on integrating diverse and flexible coping strategies (FLEX) into physical security programs [2].

2. METHODOLOGY

2.1. Event Modeling Risk Assessment Using Linked Diagrams

This work utilized Event Modeling Risk Assessment Using Linked Diagram (EMRALD) primarily to model the uncertainties in safety actions conducted to mitigate the outcomes of sabotage attacks. EMRALD is a dynamic probabilistic risk assessment model based on a three-phased discrete event simulation and comprised of discrete states. In each state are multiple events, categorizable as conditional or time-based events. Conditional events occur once specified conditions are fulfilled, whereas time-based events occur after a certain time duration has elapsed. Such time durations may be defined using probability distributions. When an event occurs, EMRALD executes certain actions modeled under that event. These actions may involve moving the simulation to another state, running an external simulation or block of programming code, or modifying certain variables.

Diagrams in EMRALD are classified in terms of overall plant level, system level, and component level. EMRALD can also model fault trees and trigger events, based on the failure/success of the fault tree's top event. In this paper, EMRALD is used in combination with a commercial force-on-force (FOF) simulation tool.

2.2. Physical Security Optimization

There are three primary aspects of physical security optimization: base case evaluation, potential strategy evaluation, and staff optimization evaluation. The steps for calculating a baseline value against which to compare the effectiveness of a protective strategy (see Figure 5) are as follows:

1. Model the plant's protection strategy.
2. Determine the model's attack scenarios.
3. Run FOF simulations and save the results for each scenario.
4. Apply defense-in-depth (DID) changes to scenarios.
5. Run DID scenarios and save the DID results.

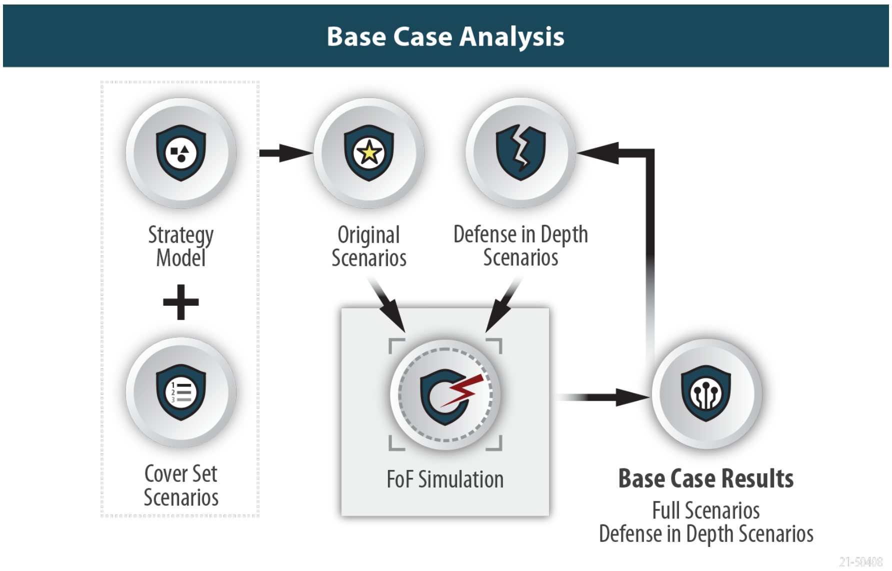


Figure 1. Flow for generating base case comparison results.

In this figure, "cover set scenario" refers to a collection of attack scenarios used for comparing various physical protection system (PPS) configurations. Cover sets consist of one or more target sets (each featuring one or more adversary pathways) selected for challenging the proposed change in the PPS. Unlike a typical analysis, in which only the top percentage of scenarios are considered, a cover set includes a variety of attack pathways, adversary strategies, and targets, thus enabling evaluation of the proposed change's impact on the security features and response of the updated PPS.

2.3. Defense-in-Depth Analysis

A typical PPS in an existing nuclear reactor yields a high effectiveness metric in FOF simulations. Therefore, modifying an element of the existing PPS posture may not only fail to significantly change the probability of effectiveness (PE), but would also carry a high degree of uncertainty. Thus, a computationally efficient method is required for analyzing the importance of a given PPS element. This is accomplished by using DID models.

DID models are modified FOF models designed to test the effectiveness of PPS elements. To fully test a defensive strategy and reduce uncertainty, cover sets require a significant number of cases featuring varied pathways, strategies, and targets. This need can be met by increasing the number of simulation runs, but doing so could be computationally expensive and possibly even onerous. Alternatively, modifying the PPS model by reducing the defensive attributes or increasing the adversary's capabilities can provide an efficient pathway for testing the PPS elements. These modifications, when applied to the baseline cover sets, are used to construct a DID model. And while there are several model changes usable to develop a DID model, the primary purpose is to verify that one simple failure or change will not significantly reduce the plant's defensive posture. Examples of modifications for constructing DID models include decreasing the guard force and/or increasing the adversary force beyond the Design Basis Threat (DBT) [4], increasing the adversary's weapon effectiveness, decreasing the defender's weapon effectiveness, and modifying the barrier delay or defensive response times. While reducing the number of responders may work in isolated cases, it is ineffective when evaluating new technology or a security posture designed to reduce the number of responders, as it prematurely removes the responder and does not provide necessary data for evaluating the "least effective post." This method is effective for changing PPS elements not located on the periphery of a site, as it is designed to highlight the most important aspects of the PPS—aspects upon which the periphery elements would have limited impact.

2.4. PPS Effectiveness

In some evaluations, simple summing of the adversary success probabilities, as determined by the different-scenario FOF simulation runs, could provide an effective comparison value if the adversary success probabilities are all low. For this work, a common risk calculation method, the minimal cut-set upper bound, was used because it enables equalization of the contributing scenarios, such that the total never exceeds 100%. The minimal cut-set upper bound is defined as follows (where P is the adversary success probability):

$$MCUB = 1 - \prod(1 - P) \tag{1}$$

An importance measure was also calculated to determine the least effective post. Calculating this importance measure entails dividing the adversary success probability by the total number of the probability scenarios. It highlights the relative significance of each attack scenario, thus helping the PPS designer determine the least effective post in a given attack scenario.

$$IM = \frac{P_A}{\sum P_A} \tag{2}$$

2.5. Personnel Optimization

Optimizing a PPS posture with regard to the number of armed responders is an iterative process, as shown in Figure 2. The iterative loop uses DID models to identify the least effective post, remove it from the model, and run the modified model in the next iteration. The loop stops when the PPS effectiveness falls below the initial/base case effectiveness, as evaluated using the DID model. The effectiveness of the final model is then compared with the effectiveness of the initial model (i.e., the one without DID).

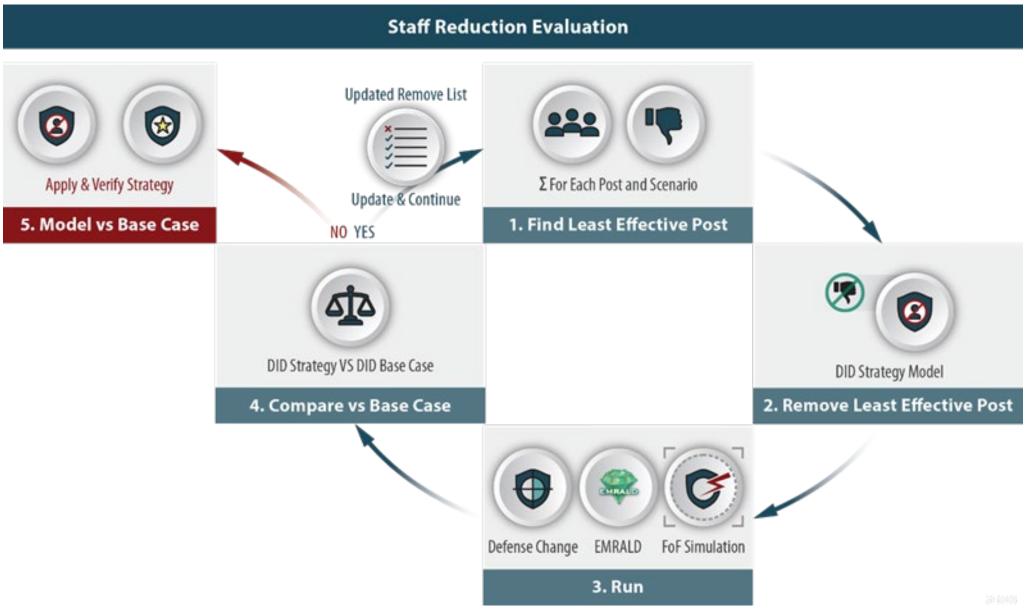


Figure 2. Process of evaluating staff reductions in alternate plant physical security strategies .

The least effective post is determined based on the significance of each attack scenario and the effectiveness of each armed responder in neutralizing adversaries in each scenario. The primary category of data used in making this determination is the number of adversaries eliminated by each post, though other criteria may also be included when deemed useful by experts . The i-th post's probability of neutralization (P_N) is given by:

$$P_{N(i)} = \frac{\sum neutralization}{\sum simulation\ runs} \tag{3}$$

where the total neutralization and total number of runs are obtained from the FOF simulation results. The i-th post's effectiveness for the j-th attack scenario is calculated by:

$$E_{(i,j)} = P_{N(i)} \times IM_{(j)} \tag{4}$$

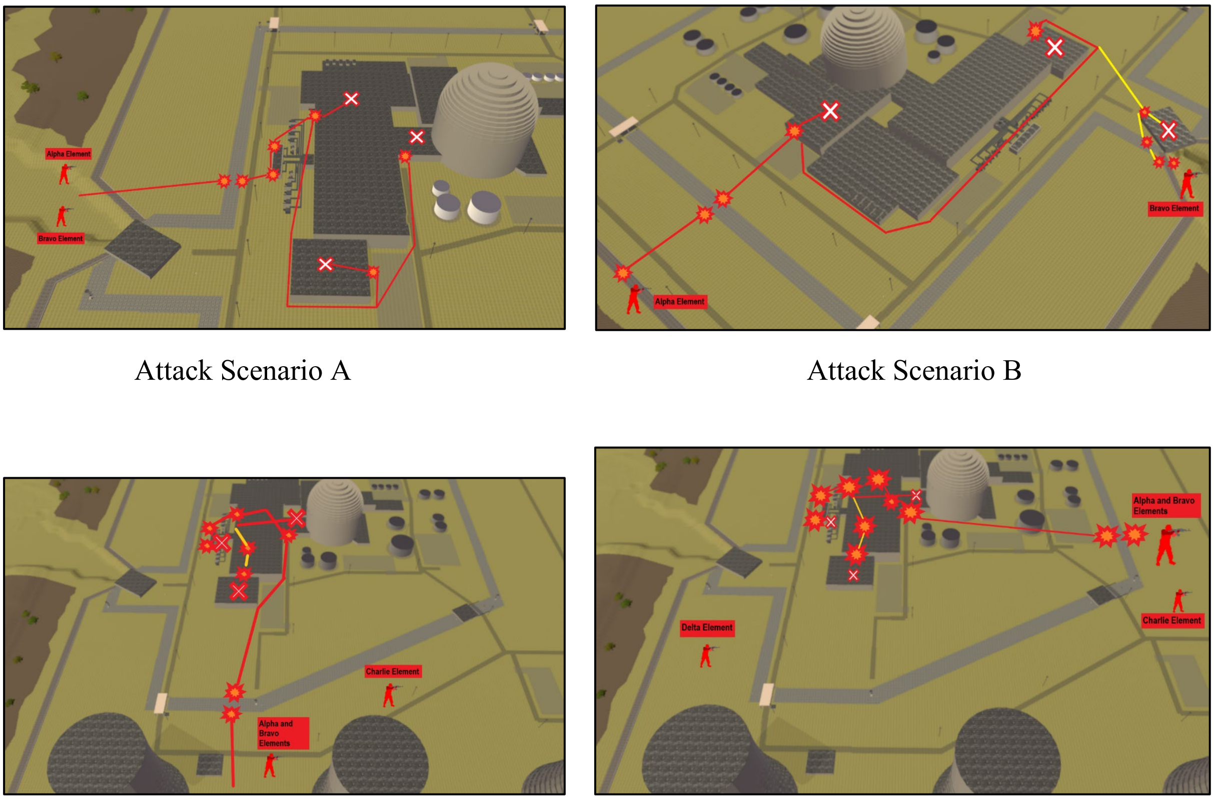
where $IM_{(j)}$ is the scenario's importance measure, given by Equation 2. The i-th post's effectiveness is the weighted sum across all attack scenarios:

$$E_{(i)} = \sum_j E_{(i,j)} \tag{5}$$

The least effective post is that which has the smallest $E_{(i)}$ of all the posts in a particular iteration.

2.6. Case Study

In this case study, hypothetical attack scenarios for a hypothetical pressurized-water reactor, the Lone Pine plant (i.e., an example used for domestic and international physical security training) [3], were developed. For illustrative purposes, a total of four attack scenarios were included in this study (see Figure 3). Two of the attack scenarios (i.e., Scenarios A and C) shared the same set of sabotage targets but had varying attack paths. In another of the scenarios, the adversaries split into two teams and attacked from two separate directions simultaneously (Scenario B). In the final attack scenario, Scenario D, the target set was attacked from yet another direction. Thus, these four scenarios represent attacks from four different directions, and for the purpose of this case study, were assumed to encompass a complete cover set.



Attack Scenario A

Attack Scenario B

Attack Scenario C

Attack Scenario D

Figure 3. Facility layout and the attack plan in the FOF model.

PPS optimization is enabled by incorporating a FLEX strategy to mitigate the adverse effects of sabotage attacks [2]. The EMRALD model, which combines the execution of the FOF simulation tool with the model of the FLEX mitigation strategies, is shown in Figure 4. The *Start* state randomizes selected parameters in the FOF simulation, such as the weapons' probability of kill, the time delay to assess an alarm, and the penalty on adversaries' movement speed, due to their unfamiliarity with the indoor areas. The *RunSimanij* state exports these parameters to the FOF model, executes the FOF simulation, reads the results, and exports the selected variables to a text file. Based on the results, the *SimanijComplete* event determines the number of intact diesel generators (DGs) and turbine driven pumps (TDPs). The *Asses_Plant_Condition* state evaluates implementable FLEX mitigation strategies and the results thereof. For example, the *Run_FLEX_EDG* event is initiated if all the design basis EDGs are sabotaged. It then transfers the simulation flow to the FLEX_DG sub-diagram. The *Check_FLEX_EDG* event is initiated if the *FLEX_DG* sub-diagram returns a value indicating successful operation of the FLEX generator. The *FLEX_Unavailable_Or_Delayed* event is initiated if the FLEX equipment is sabotaged or brought into operation later than the conservative time limit of 1 hour. This state leads to a decision as to whether the plant has been safely shut down or damaged. The *End* state writes the timing data from the EMRALD simulation into a text file for further statistical analysis.

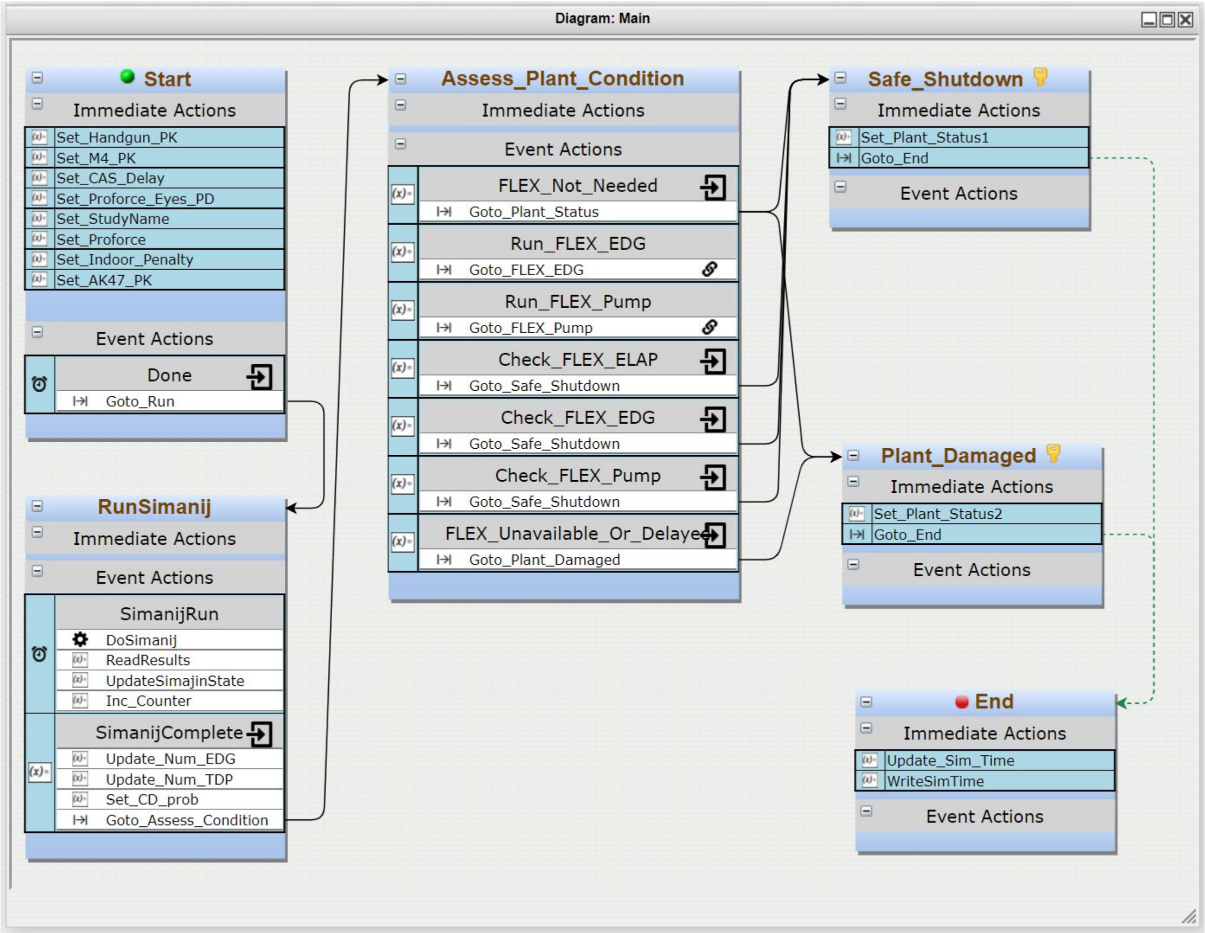


Figure 4. Main EMRALD diagram.

3. RESULTS AND DISCUSSION

The integrated FOF-FLEX model was used to simulate the initial attack. A total of 500 simulations were run for each of the four attack scenarios. The results of the first attack scenario (Scenario A) are summarized in Table 1. The scenario probability is the number of observed events divided by the total number of simulation runs (i.e., 500). The conditional core damage probability (CCDP) is the product of the FOF probability and the core damage (CD) probabilities if the respective event occurs. The CD probabilities for when the FLEX strategy is not used may be taken from plant-specific probabilistic risk assessment models. However, these values can be reasonably assumed for the hypothetical plant used in this study. Meanwhile, the CD probabilities for when the FLEX strategy is used are computed from the EMRALD simulation when the FLEX equipment fails to operate or is operated for longer than the conservative time limit of 1 hour. Some of the attack outcomes in Table 1 were avoided because the adversaries were assumed to strike target components in successions. For example, adversaries would not attack the second component on their list of targets until the first component had been sabotaged .

Table 1: CCDP Calculations for Attack Scenario A using the Initial Base Model

Scenario Number	System Availability				Number of Events	Scenario Probability	CCDP without FLEX	CCDP with FLEX
	EDG	TDP	FLEX DG	FLEX Pump				
1	Y	Y	Y	Y	384	0.768	0.768 x 1E−6	0.768 x 1E−6
2	Y	Y	Y	N	0	0	0	0
3	Y	Y	N	Y	0	0	0	0
4	Y	Y	N	N	0	0	0	0
5	Y	N	Y	Y	0	0	0	0
6	Y	N	Y	N	0	0	0	0
7	Y	N	N	Y	0	0	0	0
8	Y	N	N	N	0	0	0	0
9	N	Y	Y	Y	36	0.072	0.072 x 4E−2	0.072 x 1.54E−4
10	N	Y	Y	N	0	0	0	0
11	N	Y	N	Y	0	0	0	0
12	N	Y	N	N	0	0	0	0
13	N	N	Y	Y	77	0.154	0.154 x 1	0.154 x 1.83E−4
14	N	N	Y	N	0	0	0 x 1	0 x 1
15	N	N	N	Y	2	0.004	0.004 x 1	0.004 x 1
16	N	N	N	N	1	0.002	0.002 x 1	0.002 x 1
Total					500	1	0.1629	6E−3

Table 1 demonstrates that the FLEX mitigation strategy reduces the adversary success probability for this attack scenario. However, this only applies to that one attack scenario. The results for the whole scenario set are summarized in Table 2, which demonstrates that the FLEX strategy reduces the overall adversary success probability by two orders of magnitude. It also illustrates the probability margin obtained by utilizing backup equipment to mitigate the adverse effects of security incidents. This margin can be leveraged to optimize the PPS, especially in regard to the number of armed responders.

Table 2: Overall Probabilities of the Baseline Attack Scenarios

Scenarios	Importance Measure		CCDP	
	Without FLEX Strategy	With FLEX Strategy	Without FLEX Strategy	With FLEX Strategy
Scenario A	90.11%	96.63%	1.63E−01	6.00E−03
Scenario B	5.64%	3.22%	1.02E−02	2.00E−04
Scenario C	1.33%	0.05%	2.40E−03	2.90E−06
Scenario D	2.93%	0.11%	5.30E−03	6.60E−06
Total	100.00%	100.00%	1.78E−01	6.21E−03

DID models were investigated to analyze the effectiveness of physical security located beyond the outermost layer of protection. For this demonstration, the DID scenarios were simulated by increasing the size and attack capabilities of the adversary team. We provided details on the base and DID models in a previous publication [5].

Each post's effectiveness at neutralizing adversaries was calculated using Equations (3) and Equation (4). The results of the first iteration are shown in Figure 5, with the non-combatant posts removed. The figure shows that Scenario D is dominant, and that posts T2–T4 are seemingly less significant than the others. Figure 6 shows the total effectiveness of each post, as calculated via Equation (5), highlighting T4 as the least effective post.

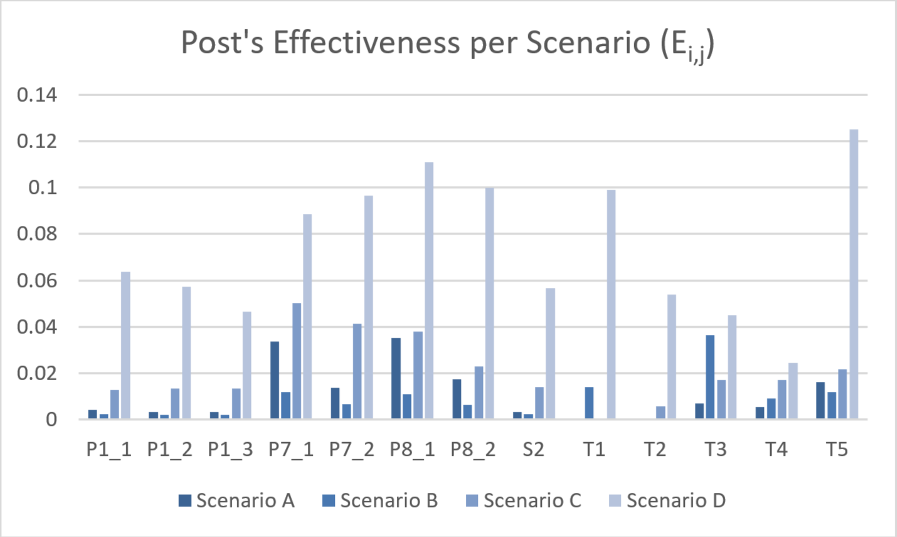


Figure 5. Each post's effectiveness per scenario for the first iteration.

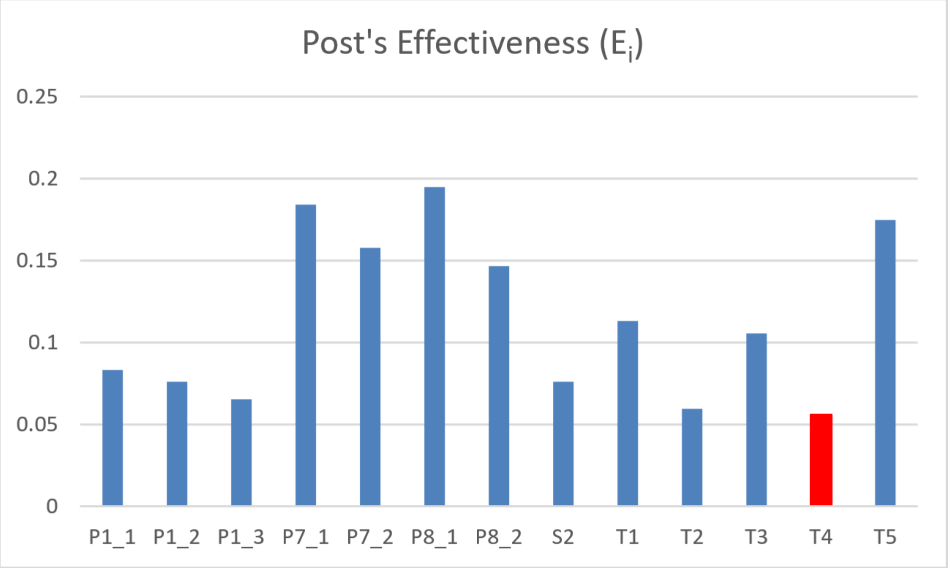


Figure 6. Each post's total effectiveness for the first iteration.

After removing T4 from the FOF model, the simulation was reiterated. With fewer posts, the PPS proved less effective. However, the margin decrease due to using the FLEX mitigation strategy can be recovered to compensate for the reduced number of posts. The least effective post can be identified and removed from the model as long as the adversary success probability is less than it would be in the absence of a FLEX strategy. Iteratively determining the least effective posts revealed that four posts could be excluded from the response force while still keeping the adversary success probability at a value below the initial one. The adversary success probability and remaining margin in each iteration is displayed in Figure 7. The figure shows that the adversary success probability when five posts are removed exceeds that of the initial value, thus that configuration is not selected.

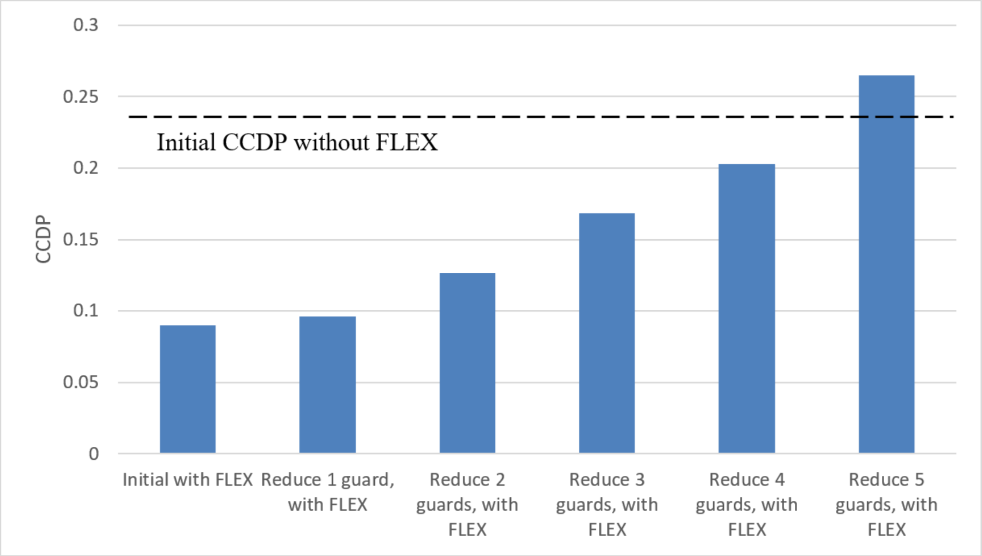


Figure 7. Adversary success probability and margin.

The optimized PPS was then validated using the initial attack capability to verify that it did not increase the adversary success probability relative to the initial PPS configuration. The result of this verification is shown in Figure 8. The metric used in the figure is the total CCDP from all attack scenarios. When the FLEX strategy is incorporated to mitigate the adverse outcomes of DBT attacks, the total adversary success probability scales down by an order of magnitude.

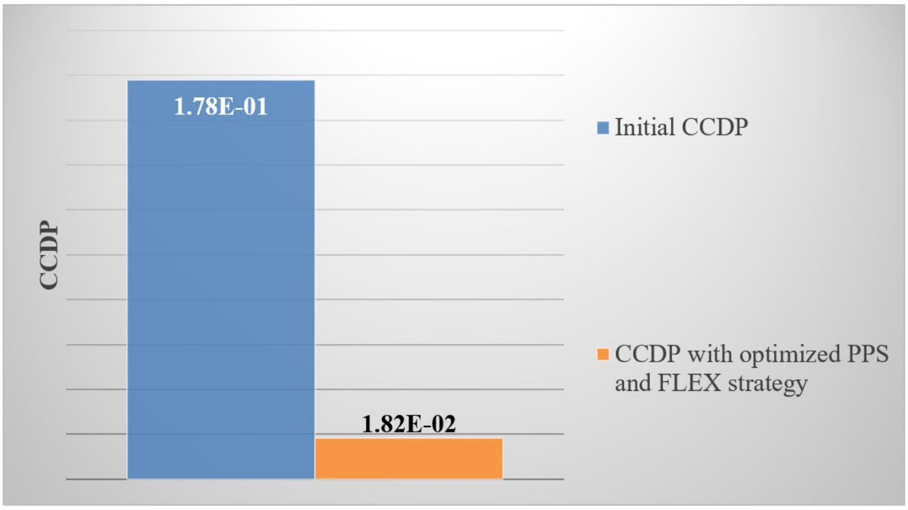


Figure 8. Adversary success probability comparison for DBT attacks

4. CONCLUSION

This paper provided an overview of a methodology for integrating FOF simulation tools with a dynamic risk simulation tool (i.e., EMRALD) to evaluate and optimize NPP physical security. The proposed methodology could be used to evaluate the effectiveness of various potential physical security enhancements and thus enable a corresponding reduction in the number of required armed responders by implementing a new strategy that affords an equivalent level of protection to the facility. One example presented in this paper entails integration of FLEX equipment into the plant protection strategy. Since this initial analysis was conducted using a generic model and hypothetical facility, additional work is required to demonstrate the methodology's usability and applicability in actual facilities.

References

[1] J. Zamanali and C. Chwasz. "*Nuclear Power Plant Security Assessment Guide*," NUREG/CR-7145, U.S. Nuclear Regulatory Commission (2013). https://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr7145/index.html.

[2] R. Christian, V. Yadav, S. Prescott, and S. St. Germain, "*Methodology and Application of Physical Security Effectiveness Based on Dynamic Force-on-Force Modeling*," presented at 2021 International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA 2021), Columbus, Ohio, 2021.

[3] D. Osborn, B. Cohn, M. Jordan Parks, R. Knudsen, K. Ross, C. Faucett, T. Haskin, P. Kitsos, and T. Noel, "*Modeling for Existing Nuclear Power Plant Security Regime*", Sandia National Laboratory (October 2019).

[4] J. Conway, N. Todreas, J. Halsema, C. Guryan, A. Birch, T. Isdanavich, J. Florek, J. Buongiorno, and M. Golay. "*Physical security analysis and simulation of the multi-layer security system for the Offshore Nuclear Plant (ONP)*," Nuclear Engineering and Design, 352, 110160. https://doi.org/10.1016/j.nucengdes.2019.110160.

[5] R. Christian, S. R. Prescott, V. Yadav, S. St. Germain, and C. P. Chwasz, "*Integration of Physical Security Simulation Software Applications in a Dynamic Risk Framework*," Idaho National Laboratory (August 2021).