INL/JOU-22-66479-Revision-0

A Dynamic Risk Framework for the Physical Security of Nuclear Power Plants

October 2022

Robby Christian, Vaibhav Yadav, Steven R Prescott, Shawn W St Germain

Changing the World's Energy Future

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/JOU-22-66479-Revision-0

A Dynamic Risk Framework for the Physical Security of Nuclear Power Plants

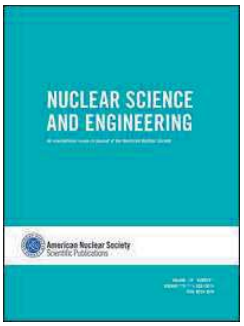
Robby Christian, Vaibhav Yadav, Steven R Prescott, Shawn W St Germain

October 2022

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517



Nuclear Science and Engineering

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/unse20

A Dynamic Risk Framework for the Physical Security of Nuclear Power Plants

Robby Christian, Vaibhav Yadav, R. Steven Prescott & Shawn W. St. Germain

To cite this article: Robby Christian, Vaibhav Yadav, R. Steven Prescott & Shawn W. St. Germain (2022): A Dynamic Risk Framework for the Physical Security of Nuclear Power Plants, Nuclear Science and Engineering, DOI: 10.1080/00295639.2022.2112899

To link to this article: https://doi.org/10.1080/00295639.2022.2112899

NUCLEAR SCIENCE AND ENGINEERING
DOI: https://doi.org/10.1080/00295639.2022.2112899

A Dynamic Risk Framework for the Physical Security of Nuclear Power Plants

Robby Christian, Vaibhav Yadav, R. Steven Prescott, and Shawn W. St. Germain*
Idaho National Laboratory, Idaho Falls, Idaho

Received March 30, 2022
Accepted for Publication August 8, 2022

Abstract — *This paper describes ongoing work within the Light Water Reactor Sustainability pathway at Idaho National Laboratory (INL) to optimize the security and cost of nuclear power plants. It introduces the dynamic risk assessment tool developed at INL, Event Modeling Risk Assessment using Linked Diagrams (EMRALD). EMRALD is leveraged to optimize the security posture of a nuclear power plant 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 are modeled in a commercially available FOF simulation tool using a hypothetical nuclear power plant facility. The simulation results provide valuable insights into possible attack outcomes, as well as the probabilistic risk of a core damage event given these outcomes. Safety mitigation procedures are modeled in EMRALD dependent on the attack outcomes by considering human operator uncertainties. The results demonstrate that the number of armed responders can be optimized, while still maintaining the same protection level as the initial security posture. The proposed modeling and simulation framework of integrating FLEX equipment with FOF models enables the nuclear power plants to credit FLEX portable equipment in the plant security posture, resulting in an efficient and optimized physical security system.*

Keywords — *Physical security, FLEX, EMRALD.*

Note — *Some figures may be in color only in the electronic version.*

I. INTRODUCTION

I.A. Background

Physical security programs at nuclear power plants (NPPs) are extremely resource intensive. Discussions with the nuclear industry have revealed that there is a need to optimize the type and amount of resources that power reactor licensees apply in meeting the Nuclear Regulatory Commission's (NRC's) physical security requirements. In other aspects of plant operations, risk-informed methods have been deployed to allow a reduction in operating costs. In the realm of physical security, there are no standard methods for risk-informed optimization of the physical protection system (PPS) that readily allow plants to evaluate alternative physical security postures that may be less resource intensive but provide an equal level of protection.

The "Nuclear Power Plant Security Assessment Guide,"[1] NUREG/CR-7145, published by the NRC, provides detailed guidance for the format and content of a security assessment at NPPs. The guidance document is widely used to optimize physical security during the design phase and in planning and executing changes and upgrades of PPSs at existing sites. NUREG/CR-7145, as

*E-mail: Shawn.StGermain@inl.gov

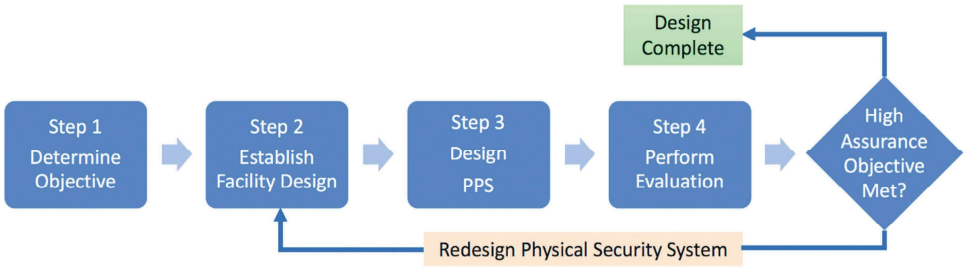


Fig. 1. Security assessment process described in NUREG/CR-7145.

well as the accompanying document, SAND-2007-5591, "Nuclear Power Plant Security Assessment Technical Manual,"[2] provide a detailed methodology for performing an assessment of physical security system effectiveness. Figure 1 shows the four-step security assessment process described in NUREG/CR-7145 (Ref. 1):

Step 1. Determine objective. The objective of a physical security system is to protect the plant against radiological sabotage as required by Title 10 of the *Code of Federal Regulations* (10 CFR) Part 75.55 (b) as defined in 10 CFR Part 73.1 (Ref. 3). The NRC defines the design-basis threat (DBT) within nonpublic regulatory documents as a set of adversary characteristics and capabilities, such as force size, equipment, weapons, and tactics.[4] For a given DBT scenario, there can be variations based on variability in target sets, entry points, adversary numbers, tactics, and other plant-specific characteristics. The NRC has developed a standard set of scenarios[5] that cover a range of DBT characteristics that provide a basis for the assessment of a PPS design.

Step 2. Establish facility design. An initial facility design is used to establish the protective strategy. The systems, structures, and components that must be protected to prevent significant core damage (CD) and spent fuel sabotage are identified through a target set analysis. A target set is the combination of equipment or operator actions which, if prevented from performing their intended safety function or prevented from being accomplished, would likely result in significant CD or loss of spent fuel pool coolant inventory and exposure of spent fuel, barring extraordinary actions by plant operations.[6]

Step 3. Design PPS. The PPS at a NPP is a combination of structures, systems, equipment, personnel, and procedures with the combined aim of protecting the plant against the DBT. This step characterizes the different elements of the PPS, such as delay elements, detection and assessment equipment, response forces, layout of the PPS elements at the site, and the procedures for the protective force response.

Step 4. Perform evaluation. The physical security performance evaluation is performed in three broad steps:

1. Apply NRC-developed scenarios and evaluate PPS.
2. Analyze scenarios to ensure adversary actions are within DBT capabilities and credible.
3. Analyze scenarios to ensure barrier delay times and protective force actions are credible.

I.B. Problem Description

Given a specific facility model, an attack pathway can be evaluated by simplifying the facility in an adversary sequence diagram (ASD) model.[7] Figure 2 illustrates an ASD of a hypothetical facility. The ASD transforms

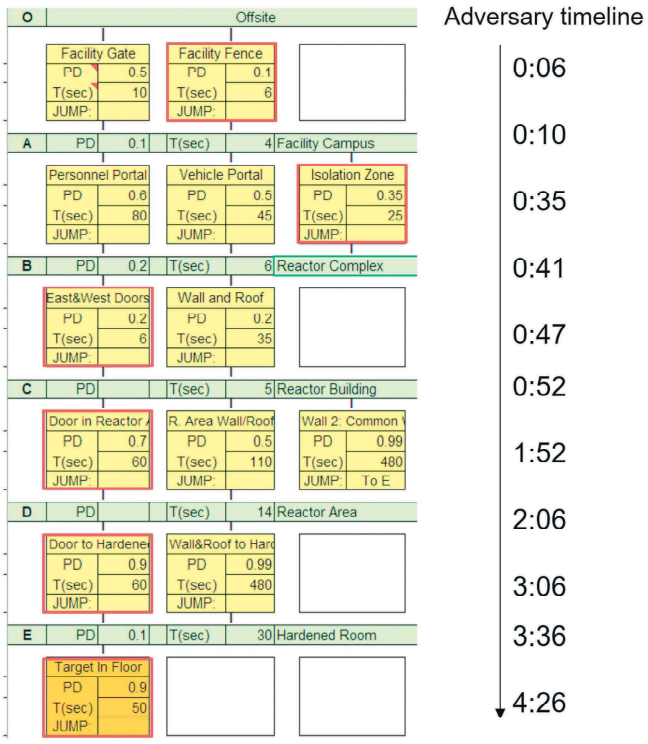


Fig. 2. Adversary sequence diagram.

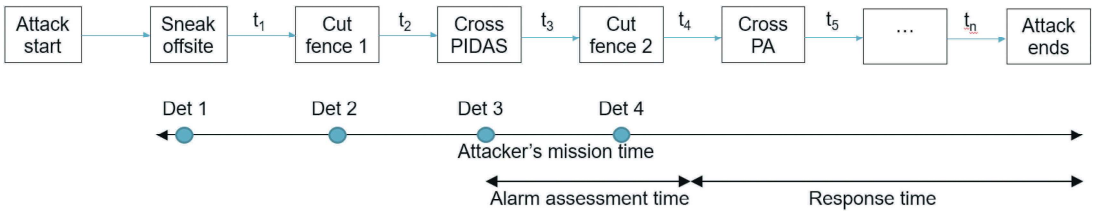


Fig. 3. Attack timeline.

the facility layout into a diagram comprised of areas and barrier blocks separating the areas. Each block in the diagram is assigned a detection probability (P_D) and traversal time T. These values are evaluated independently for each area/barrier and are typically conservative. An attack timeline can be created based on the ASD diagram, as illustrated in Fig. 3. Based on the competition between adversary time and responder time, a critical detection point (CDP) is designated beyond which the intrusion alarm system is not credited in the PPS because it would have been too late to intercept the adversary in a timely manner.

The cumulative probability for the PPS to intercept adversaries before they finish their attack is given by the probability of interruption (P_I),

$$P_I = 1 - \prod_1^3 (1 - P_D)_i \ . \tag{1}$$

The PPS effectiveness is formulated as

$$P_E = P_I \times P_N \ , \tag{2}$$

where P_N is the probability of the response force neutralizing the attackers. The advantages of this methodology rely on its simplicity and ease of use. However, it uses conservative assumptions, such as simplification of uncertainties, statistical independence, and conservative values, for the performance of the intrusion detection assessment systems.[8] This conservatism may result in an overly conservative PPS design. Furthermore, it assumes that the security objective is defeated when the adversaries have completed their tasks. NPPs are complex industrial systems employing redundant safety mechanisms to prevent accidents. There is an elapsed time before the nuclear core may be damaged after adversaries disable targeted components of the plant. Within this timeframe, there are mitigation actions that can be done to prevent the adverse effect of an attack, either by using the design-basis safety systems or additional actions.

Existing NPPs have diverse and flexible coping strategies and guidelines[9] (FLEX) to mitigate accident conditions under an extended loss of alternating-current (ac) power (ELAP) and the loss of normal access to the ultimate heat sink conditions. This existing strategy may be leveraged to safely shut down the reactor and maintain decay heat removal in case of a sabotage attack. The NRC has recently issued a revision to Regulatory Guide 5.76 (Ref. 10) that allows crediting of local law enforcement through the implementation of the reasonable assurance of protection time (RAPT) concept. RAPT provides a pathway to establishing an end time to security events and a timeline for the crediting of operator actions after a security event. This work proposes an evaluation methodology that incorporates these operator actions and also optimization of the security posture to support the objective of physical security (i.e., prevention of significant CD and spent fuel sabotage). This paper expands our previous paper[11] by utilizing the risk margin estimated from the dynamic methodology and operator actions to optimize the number of armed responders.

I.C. Related Work

This subsection presents a brief literature review of significant studies performed for physical security of NPPs:

1. Garcia[12] explains the design and evaluation process outline (DEPO) of the PPS methodology. It details the building blocks of a PPS, which include detection, delay, and response, and the formulation to calculate risk as a function of stochastic attack, PPS effectiveness, and the consequence of a successful attack.

2. Wely and Chetaine[13] applied the DEPO methodology to analyze a PPS performance by using the Estimate of Adversary Sequence Interruption (EASI) model. The EASI model analyzes attack paths and the associated detection and delay elements along the path to obtain the overall probability of interrupting the adversaries before they complete their mission. Wely and

Chetaine discuss insider and outsider attack scenarios in a simple and hypothetical facility layout.

3. Wadoud et al.[14] performed research similar to Wely and Chetaine by using DEPO and EASI, and added a discussion on the P_N in addition to the P_I Wely and Chetaine addressed. Wadoud et al. used the ASSESS neutralization model to estimate P_N. A hypothetical research reactor facility is presented to show the applicability of the methodology.

4. Zou et al.[15] took EASI a step further by using it with the Absorbing Markov Chains (AMC) method to establish and simulate state chains, with transition probability obtained from EASI. The AMC/EASI approach allows a vulnerability learning method for the analysis of adversary paths. The process depends on the development of AMC models that resemble the ASD, matrix of transition probability values, and matrix operations. The vulnerability learning process is a continuous-time, complicated, and dynamic decision process for the adversary. A case study of a minimum PPS system is presented in the paper.

5. Setiawan et al.[16] developed a multipath analysis of physical protection systems (MAPPS) to analyze PPS effectiveness. While EASI is limited to a single path analysis only, MAPPS can analyze multiple paths and determine the most vulnerable path. The most vulnerable path determination by MAPPS uses the concept of CDP. A hypothetical facility model was developed and various attack vectors were developed to test the MAPPS tool.

6. Zou et al.[17] proposed a different path-finding methodology than what MAPPS proposed by using a heuristic path-finding methodology called HPEP. The methodology takes the P_D and P_I as heuristic information to analyze vulnerability. It modifies the A* algorithm for the analysis of the adversary behavior and uses the common A* algorithm to calculate a fast path. It is able to find the shortest path for the responders to interrupt the adversary.

7. Silva et al.[18] developed a virtual reality tool to allow users to interact with the virtual facility of the Brazilian nuclear research center. It is a three-dimensional model with a high degree of fidelity. The avatars inside the model can move and interact in real time. The tool was developed to aid in planning security action strategies.

These previous research efforts show the general approach used in designing and evaluating PPS in a nuclear facility, i.e., by using computational models. Some research focuses on finding certain attack paths of interest, such as the most vulnerable path and shortest path. They are beneficial in providing insights into PPS effectiveness, however, they are not immediately applicable to the research objective in this current work. This work investigates the effectiveness of the FLEX mitigation strategy in reinforcing a nuclear plant's safety, which requires a dynamic analysis methodology not available in previous research. FLEX inclusion makes the target set more robust, such that it is more difficult for adversaries to sabotage a NPP with the same attack capability.

II. METHODOLOGY

Figure 4 illustrates a detailed look at a postulated attack timeline. The center timeline represents the initial attack plan. When adversaries infiltrate through the owner-controlled area, they may be seen by armed guards on patrol, in which case the adversaries may retreat and resume the attack another time or they may open fire at the guards. The time distribution to cut the first (nuisance) fence in the planned condition is $P(t_1)$; however, if the adversaries are under fire, this action may take a longer time as $P(t_{1a})$. When adversaries cut the first fence, the cutter may break, and they may cancel the attack altogether or they may climb the fence. Climbing

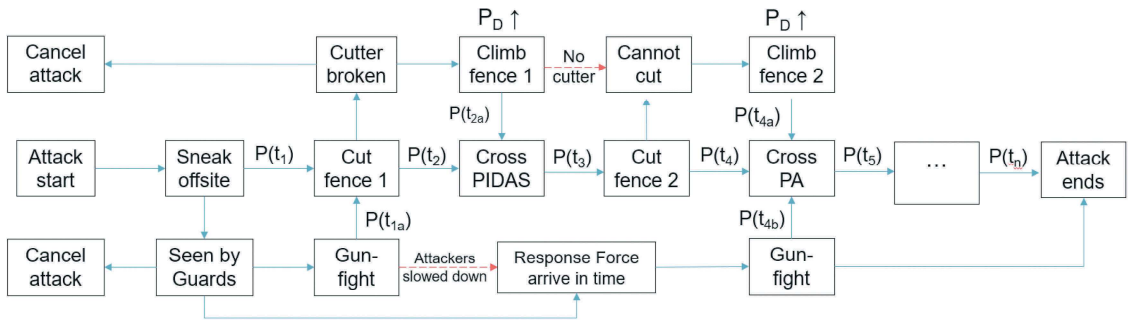


Fig. 4. Possible variations of an attack plan.

the fence may increase the P_D and alter the task completion time. Since the cutter has failed, they may likewise climb the second fence (protected area barrier) instead of cutting it as planned, due to the failure of that equipment. If the adversaries are sufficiently delayed, the response force may arrive while they were still in the isolation zone of the perimeter intrusion detection and assessment system, further delaying penetration of the second fence.

These possible scenarios as described imply that despite the conservative assumptions of the attackers' capabilities, there are various ways an attack plan can go wrong. Furthermore, the different ways a plan goes wrong may affect the next steps of attack or intervention actions. Therefore, there are dynamic dependencies among the steps. These dependencies mean that the mission time may not be constant. These are the implications of introducing realism into the evaluation of PPS, which are different than the assumptions employed in the static methodology described in the previous section.

The PPS effectiveness in the dynamic methodology is conceptually formulated as

$$P_E = P_D|A \times P_t|D \times P_N|t \ , \tag{3}$$

where $P_D|A$ is the probability of detection, which is dependent upon the adversary's action, $P_t|D$ is the probability of timely interception, which depends on the intrusion detection event, and $P_N|t$ is the probability of neutralization, which depends on the time of the response force's arrival. If the response force arrives early, they may set up a defensive position that gives them an advantage to neutralize the incoming adversaries, as opposed to when they arrive later and are forced to engage while running. The dynamic dependencies in these variables are evaluated by simulating the uncertainties in the attack plan using a force-on-force (FOF) simulation tool. In addition to modeling dynamic dependencies in the FOF phase to reduce conservatism, this research also models dynamic uncertainties in operators' actions to mitigate the sabotage attack by using a dynamic modeling tool described in the following subsection.

II.A. Event Modeling Risk Assessment Using Linked Diagrams

In this work, Event Modeling Risk Assessment using Linked Diagram (EMRALD) is utilized primarily to model the uncertainties in safety actions to mitigate the outcomes of a sabotage attack. EMRALD is a dynamic probabilistic risk assessment (PRA) model based on a three-phased discrete event simulation. It is comprised of discrete states. In a state, there are multiple events that are categorized into conditional events and time-based events. Conditional events occur when the specified conditions are fulfilled. Meanwhile, time-based events happen after a certain time has elapsed, which 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 a block of programming code, or modifying certain variables.

Diagrams in EMRALD are classified into several levels (i.e., overall plant level, system level, and component level). EMRALD can also model fault trees and trigger events based on the failure or success of the fault tree's top event. In this paper, EMRALD is used together with a commercial FOF simulation tool.

II.B. Physical Security Optimization

This section describes the process to evaluate and optimize the PPS when implementing changes in equipment, staffing, strategy, or the inclusion of operator actions, to include the implementation of FLEX. This process consists of three main parts: base case evaluation, potential strategy evaluation, and staff optimization evaluation. The following steps to calculate a baseline value for comparison from a change in protective strategy, as shown in Fig. 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.

Further explanations are given in the following subsections.

II.B.1. Cover Set Scenarios

To demonstrate there is no reduction in PPS effectiveness, a baseline probability of effectiveness (P_E) value is first estimated from a plant's current defensive posture described in the NRC-approved site security plan. This is accomplished by modeling in a FOF simulation tool capable of capturing the strategies and procedures established by the NPP. Expert judgment, past FOF exercises, and software tools should be used to identify a cover set of scenarios.

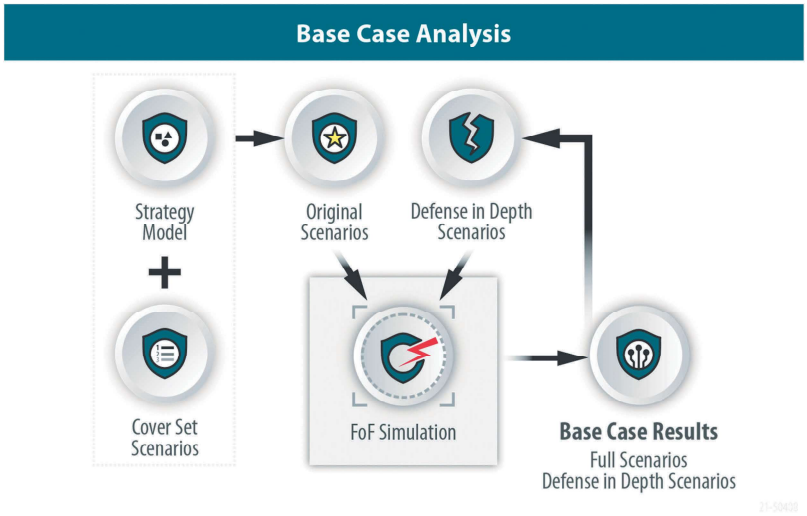


Fig. 5. Flow for creating base case comparison results.

A cover set scenario in this study is defined as a grouping of attack scenarios used to compare PPS configurations. Cover sets are comprised of one or more target sets (each with one or more adversary pathways) chosen to challenge the proposed change in the PPS. Unlike a typical analysis where only the top percentage of scenarios are considered, the cover set includes a variety of attack paths, adversary strategies, and targets in order to evaluate the impact of the proposed change on the security features and response in the revised PPS. Attack scenarios with low probability of PPS success should be included, and only similar routes with equal or smaller DBT adversary characteristics should be excluded.

II.B.1.a. PPS Effectiveness and Comparison Calculation

The effectiveness of the PPS, conditional on an attack occurring, can be defined as the PPS success probability of the scenario with the highest probability of adversary success, as only one attack scenario can occur at a time. PPS effectiveness may also be measured by the probability for adversary success, in which a lower adversary success denotes a more effective PPS. For the purpose of this analysis, we frame PPS effectiveness in terms of adversary success. A proper PPS analysis will evaluate multiple potential attack scenarios. Evaluating each potential attack scenario will result in a ranking of scenarios based on the likelihood of the adversary's success.

When modifications are made to a PPS, it is possible the probability of adversary success may go down for some scenarios and go up for other scenarios. It is arguable that PPS changes that result in increases to the adversary success probability to anything equal to or below the probability of the previous largest adversary success probability scenario do not significantly decrease the PPS's effectiveness. However, it is also arguable that if the adversary chooses an attack strategy not consistent with the largest adversary success probability scenario, due to lack of knowledge or other factors, then a change made that increased that scenario probability in actuality reduced the PPS's effectiveness against that specific attack path. In the future, a statistical weighting system based on the adversary success probability could be used to determine an overall value for comparison. For simplicity and conservatism, a cumulative measure was used for comparing changes in this work. While a cumulative process does not represent the actual probability level, it provides a single base case value for a cover set for comparative evaluations, such as the removal of responders, while still ensuring the PPS contributions to those scenarios can be effectively captured.

In some evaluations, simple summing of the adversary success probabilities, determined by the different scenario FOF simulation runs, could provide an effective comparison number if the adversary success probabilities are all low. For this work, a common risk calculation method, Minimum Cut Set Upper Bound (MCUB), was used since it provides a method to equalize the contributing scenarios so that the total never exceeds 100% (Ref. 19). As shown by the example in part (A) in Table I, when using relatively few small probabilities, the sum and MCUB have similar values. However, with more or larger probabilities, as shown in part (B) in Table I, the MCUB provides a better comparison number. MCUB is defined as

$$\text{MCUB} = 1 - \prod (1 - P) \ , \tag{4}$$

where P is the adversary success probability.

An importance measure (IM) is also calculated to determine the least effective post. The importance measure for each scenario is the adversary success probability for that scenario P_A divided by the sum of all the scenarios' probabilities $\sum P_A$. It informs the relative significance of each attack scenario, which helps the PPS designer decide the least-effective post corresponding to the attack scenario's significance,

$$\text{IM} = \frac{P_A}{\sum P_A} \ . \tag{5}$$

II.B.1.b. DID Analysis

The PPSs in existing NPPs typically yield a high P_E in a tabletop and FOF simulation analysis. For that reason, modifying an element of the existing PPS posture may not result in a significant change in P_E and would have a high degree of uncertainty. Therefore, there needs to be a computationally efficient method to analyze the importance of a PPS element. This is done through the use of DID models.

Defense-in-depth models are modified FOF models designed to test the effectiveness of PPS elements. To fully test the defensive strategy and reduce uncertainty, cover sets need to have a significant number of cases with varied pathways, strategies, and targets. This may be accomplished by increasing the number of simulation runs, but that could be computationally expensive and onerous. Alternatively, modifying the PPS model by reducing the defensive attributes or increasing the adversary's capabilities can provide an efficient pathway to test the PPS elements. These modifications applied to the baseline cover sets are used to construct a DID model. While there are several model changes that can be used to develop a DID model, the primary purpose is to verify that one simple failure or change will not cause a significant reduction in the defensive posture.

Some examples of model changes for constructing DID models include decreasing the guard force and/or increasing the adversary force beyond the DBT (Ref. 19), increasing the weapon effectiveness of the adversary, decreasing the weapon effectiveness of the defender, and modifying barrier delay or defensive response times. While reducing the number of responders may work in isolated cases, this will not be effective when evaluating new technology or a security posture designed to reduce the number of responders, as this would remove the responder prematurely and not provide the data needed for evaluating the least effective post. This method is effective for changing PPS elements that are not on the periphery of a site, as the method is designed to highlight the most important aspects of the PPS, and the periphery elements would have limited impact.

TABLE I

(A) Example Base Case and (B) Example Change Case

(A) Example Base Case			(B) Example Change Case		
Scenario	Adversary Success Probability	Importance Measure	Scenario	Adversary Success Probability	Importance Measure
A	0.2	74.91%	A	0.2	12.20%
B	0.05	18.73%	B	0.2	12.20%
C	0.01	3.75%	C	0.4	24.39%
D	0.001	0.37%	D	0.4	24.39%
E	0.001	0.37%	E	0.2	12.20%
F	0.001	0.37%	F	0.2	12.20%
G	0.001	0.37%	G	0.01	0.61%
H	0.001	0.37%	H	0.01	0.61%
I	0.001	0.37%	I	0.01	0.61%
J	0.001	0.37%	J	0.01	0.61%
	Sum	Sum		Sum	Sum
	0.267	1.0000		1.64	1.0000
	MCUB			MCUB	
	0.252851026			0.858354355	

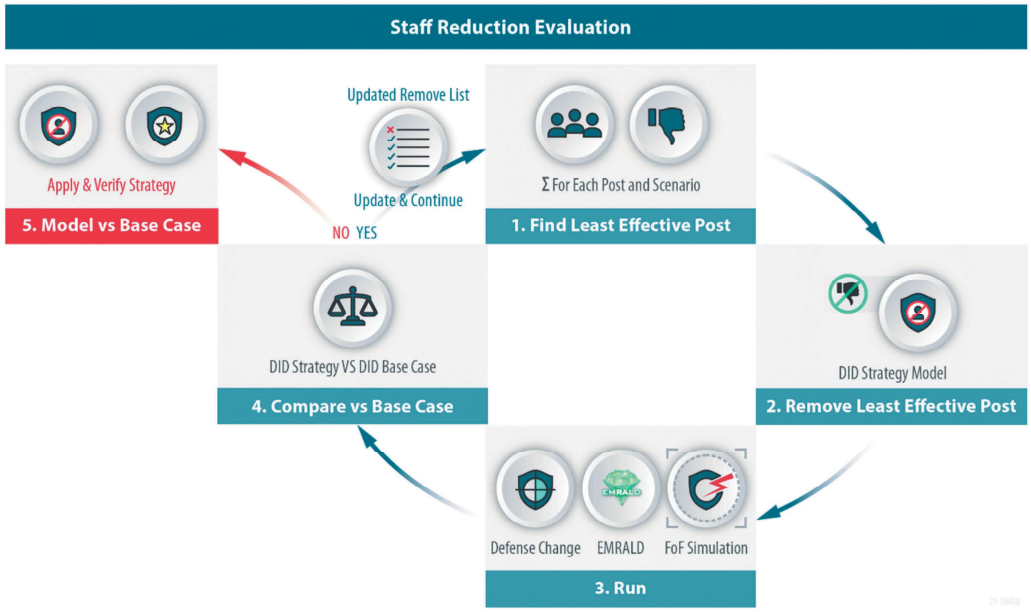


Fig. 6. Process to evaluate staff reduction for a strategy change.

II.B.2. Personnel Optimization

The five main steps to optimize the number of armed responders are outlined in Fig. 6 and described here. This is an iterative process using the DID model and stops once the criteria have been met. The following summarizes the loop process, and the subsections give details and specifications for some steps:

1. Use the current modified strategy DID results to determine which post was the least effective over the scenario.

2. Remove the identified least effective post from the cover set scenarios in the DID changed strategy model.

3. Run the FOF simulation of the modified cover sets [with the defense changes and post(s) removed] to determine the effectiveness of the new model.

4. Compare the changed strategy DID model results with the newly removed post(s) to the DID base results:

   a. If the proposed change result is as good as or better than the DID base model result, iterate starting again at step 1.

   b. Otherwise, the proposed change result is worse than the DID model, and the staff reduction selection is complete, so exit the staff reduction loop by moving to step 5.

5. Apply the remove list to the original potential strategy model. Run and verify that the results are less than the original base case model.

Once the iterative process is complete in step 5, the result of the staff reduction evaluation is the remove list, which contains the posts that can be eliminated if the potential strategy is implemented. This process takes a conservative iterative approach and does not account for the possibility of correlated posts where a combination of possibly more effective responders could be less impactful than iteratively removing the worst one at a time.

II.B.2.a. Evaluating the Least Effective Post

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 the attack scenarios. The primary data for evaluating the least effective are the number of adversaries eliminated by each post, although other criteria may also be included as deemed useful by expert judgment. An i'th post's P_N is given by

$$P_{N(i)} = \frac{\sum neutralization}{\sum simulation\ runs} \quad , \tag{6}$$

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

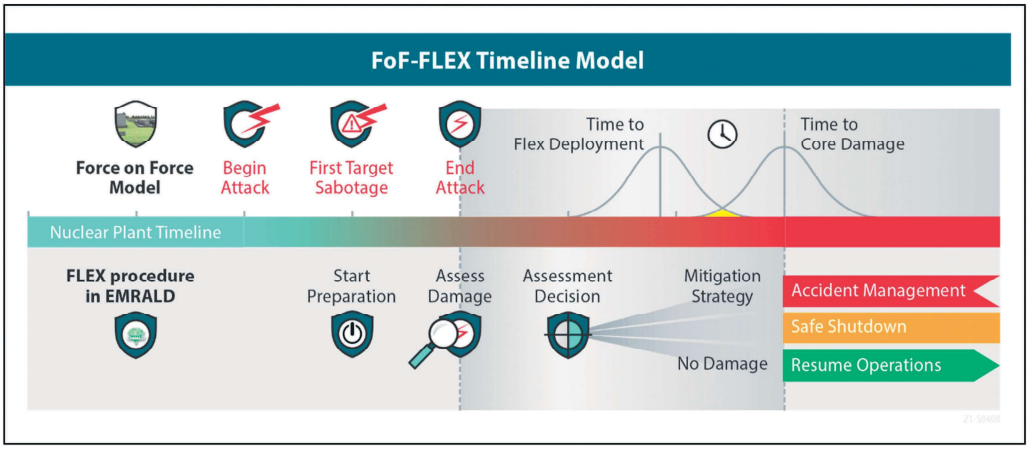


Fig. 7. FOF-FLEX integration framework.

$$E_{(i,j)} = P_{N(i)} \times IM_{(j)} \ , \tag{7}$$

where IM(j) is the scenario's importance measure given in Eq. (5). The i'th post's effectiveness is the weighted sum across all attack scenarios:

$$E_{(i)} = \sum\nolimits_j E_{(i,j)} \ . \tag{8}$$

The least effective post is the post having the minimum $E_{(i)}$ of all the posts in a particular iteration.

II.C. Integration of Physical Security with FLEX

Figure 7 illustrates the dynamic framework overview of FOF and FLEX model integration. The integration starts with the FOF simulation being conducted using a commercial FOF software. The FOF simulation provides the attack timeline data as well as the targets' conditions at the end of the attack. These data are read by EMRALD to determine the proper timing to start the preparation of the FLEX portable equipment. This stage may include communication and coordination with field personnel, equipment mobilization, staging, and connection. The mobilization and staging phase may be skipped if the FLEX equipment is prestaged. Dynamic uncertainties of the FLEX preparation, as modeled in EMRALD, create a statistical distribution of the timeline outlining when the FLEX equipment is operational. At the end of the attack scenario, EMRALD fetches the list of targets and their conditions from the FOF simulation output. The EMRALD model uses these data to decide the applicable mitigation strategy, as needed. If the attack is not successful at all, the plant may safely shut down and resume its normal operation depending on the plant's procedure. Meanwhile, if several components or equipment are sabotaged but the plant still retains its design-basis safety functions as maintained by intact redundant or standby components, the mitigation is done using the design-basis systems. Last, mitigation strategies using FLEX equipment are conducted when the safety functions of the design-basis systems are lost due to the sabotage attack. The execution of this FLEX strategy depends on which safety functions are lost after the attack.

II.D. Case Study

A case study is described in this section to demonstrate the applicability of the FOF-FLEX integration model. A hypothetical attack scenario of a hypothetical pressurized water reactor (PWR) Lone Pine plant, which is an example used for domestic and international physical security training, was developed in this case study. This case study does not use any plant proprietary data or information, and the targets and adversary characteristics are hypothetical and bear no resemblance to an actual site or the DBT adversary characteristics.

In the hypothetical attack scenario, a group of adversaries attempts to cause a radiological release by sabotaging the PWR plant's power supply and its ultimate heat sink capabilities. The attack follows the event progression highlighted in red in Fig. 8, which is adopted from a station blackout (SBO) event tree for a PWR plant.[20]

Target locations and the attack pathways to inflict the aforementioned CD progression are shown in Fig. 9. An adversary sets explosives at an unmonitored grid tower outside of the NPP complex to cause a loss-of-offsite-power event. Meanwhile, two groups of armed adversaries enter the complex to sabotage the emergency diesel generators (EDGs) to cause a SBO event and damage the turbine-driven pumps (TDPs) to disable the plant's passive heat

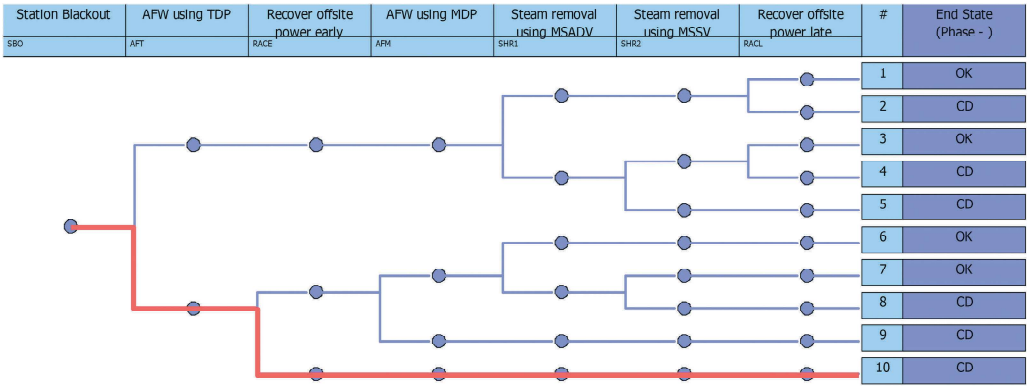


Fig. 8. Sabotage scenario to inflict CD.

removal capability. Adversaries then proceed to sabotage the prestaged FLEX diesel generator (DG) and FLEX pump to disable the plant's mitigation strategy completely. The plant has its physical protection program in place, consisting of the intrusion detection system, delay barriers, and both the stationary and mobile response force. These protection elements are not shown in Fig. 9 to provide visual clarity of the attack path and target locations. The PRA models show that if all of these targets are sabotaged, the nuclear plant will experience the CD state within 1 h (Ref. 20).

This study incorporates Simajin developed by Rhinocorps as the third-party commercial FOF tool. The attack paths were predesigned in the model and remained the same throughout the iterations. The adversaries' numerical parameters follow the default parameters in Simajin since the attack scenarios are hypothetical. It is important to note that in a realistic model, the numerical parameters should adequately correlate to the adversaries' skill, knowledge, and training levels. For example, a common adversary force may assume their tools will work, while a more experienced adversary force will use high-quality tools with contingency plans for their missions. A trained adversary will also perform tasks faster than an untrained one. The compounded probabilities and action timings throughout the attack plan may change the final outcome. However, the study of appropriate FOF numerical parameters is beyond the scope of the current work.

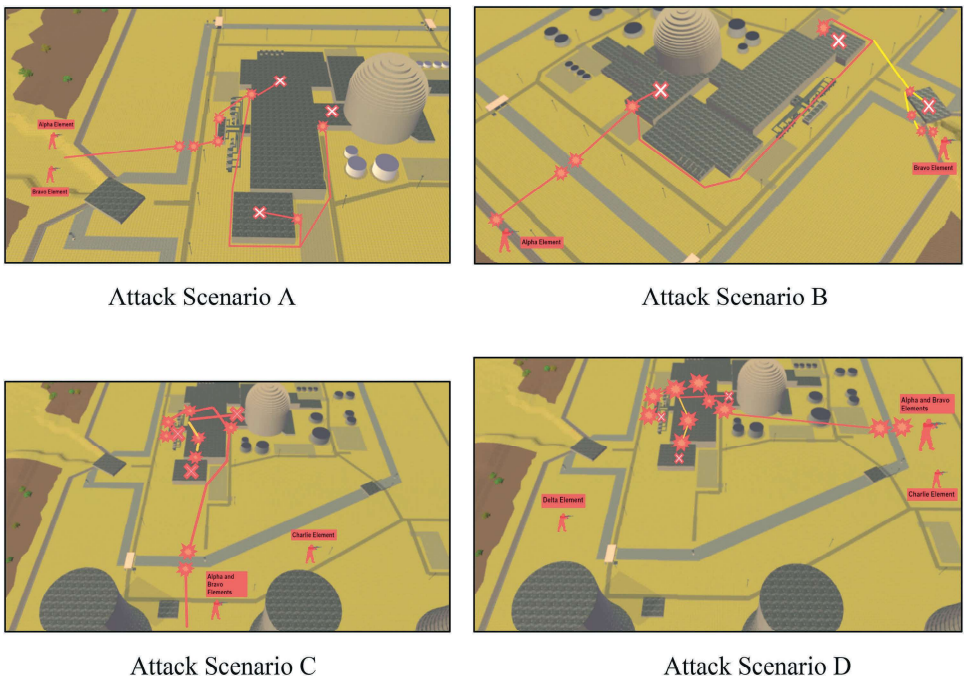


Fig. 9. Facility layout and attack plan in the FOF model.

Simajin, as well as many other FOF simulation tools, models human actors in a statistical manner in the sense that they can perform certain actions with certain success probabilities. The approach of modeling human actors using statistical randomness may not fully capture the capability of deliberate human decision making, which is driven by a rational mind and psychological aspects. A tabletop scenario review prior to modeling the attack plan in the FOF computer model can help to incorporate such considerations in the model. However, further studies to model human actors differently in FOF simulations may be useful to improve confidence in the FOF results. Such a fundamental analysis is currently beyond the scope of this paper.

Multiple attack scenarios were investigated to analyze the overall plant physical security posture. For the purpose of illustration, a total of four attack scenarios were included in this study, as shown in Fig. 9. Two attack scenarios, scenario A and scenario C, having the same set of sabotage targets but varying attack paths, were developed. An additional attack scenario was created in which the adversaries split into two teams attacking from two separate directions simultaneously (scenario B). In another attack scenario, scenario D, the adversaries attack the target set from another direction. The four scenarios represent attacks from the four different directions. For this case study, it is assumed these few scenarios are a complete cover set.

A list of all possible outcomes from the attack scenarios is shown in Table II, incorporating FLEX equipment in the target set. If adversaries fail to sabotage any one of the target systems in the target set, as indicated in the first outcome, the plant will shut down safely. Meanwhile, if the plant loses several of its design-basis safety systems, as listed in outcomes 5 through 12, FLEX strategies are initiated to shut down the reactor. If the corresponding FLEX equipment that provide backup safety functions is sabotaged, the reactor core is assumed to be damaged. Similarly, if all design-basis safety systems are sabotaged, the FLEX ELAP strategy is assumed successful if all the necessary backup equipment is intact.

II.E. FLEX Implementation in EMRALD

Figure 10 shows the main diagram of the EMRALD model combining the execution of the FOF simulation tool and the model of FLEX mitigation strategies. The *Start* state randomizes selected parameters in the FOF

TABLE II

Possible Attack Outcomes

Number	System Availability				Mitigation Strategy
	EDG	TDP	FLEX DG	FLEX Pump	
1	✓	✓	✓	✓	Safe shutdown
2	✓	✓	✓	X	Safe shutdown
3	✓	✓	X	✓	Safe shutdown
4	✓	✓	X	X	Safe shutdown
5	✓	X	✓	✓	FLEX pump strategy
6	✓	X	✓	X	N/A[a] (CD)
7	✓	X	X	✓	FLEX pump strategy
8	✓	X	X	X	N/A[a] (CD)
9	X	✓	✓	✓	FLEX generator strategy
10	X	✓	✓	X	FLEX generator strategy
11	X	✓	X	✓	N/A[a] (CD)
12	X	✓	X	X	N/A[a] (CD)
13	X	X	✓	✓	FLEX ELAP strategy within 1 h
14	X	X	✓	X	N/A[a] (CD)
15	X	X	X	✓	N/A[a] (CD)
16	X	X	X	X	N/A[a] (CD)

[a]N/A = Not Applicable.

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 selected variables to a text file. Based on the results, the *SimanijComplete* event determines the number of intact DGs and TDPs. The *Assess_Plant_Condition* state evaluates FLEX mitigation strategies to implement and their results. For example, the *Run_FLEX_EDG* event is initiated if all the design-basis EDGs are sabotaged. It transfers the simulation flow to the FLEX_DG subdiagram. The *Check_FLEX_EDG* event is initiated if the *FLEX_DG* subdiagram returns a value that indicates the success of the FLEX generator's operation. The *FLEX_Unavailable_Or_Delayed* event is initiated if the FLEX equipment is sabotaged or brought into operation later than a conservative time limit of 1 h. This state leads to the decision of whether the plant is safely shut down or damaged. The *End* state writes the timing data from the EMRALD simulation into a text file for further statistical analysis.

Table III shows the procedure to implement a FLEX strategy in this case study. Steps in this procedure were categorized into preparation and execution stages of the FLEX strategy. Preparatory actions were done prior to executing the FLEX mitigation strategy, as illustrated in the "Start Preparation" step in Fig. 7. After the FOF simulation is completed, an assessment is done to determine the plant condition. Based on the damages to the plant after the attack, the appropriate FLEX strategy is performed, following the execution actions in Table III.

Some of the actions listed in Table III are modeled in the FOF simulation, such as the FLEX operators moving to their respective equipment. The delay prior to mobilization, which includes steps 1, 2, and 3, and the delay in preparing the equipment, which includes steps 5, 9, 11, and 15, are in the FOF simulation. The remainder of the FLEX mitigation actions are modeled in EMRALD as shown in Figs. 11 and 12 for the FLEX generator and FLEX pump, respectively.

In the FLEX generator strategy, the *MCC_preparation* stage samples the time required for a FLEX operator to connect the FLEX cables to the 480-V motor control center (MCC). After the cables are

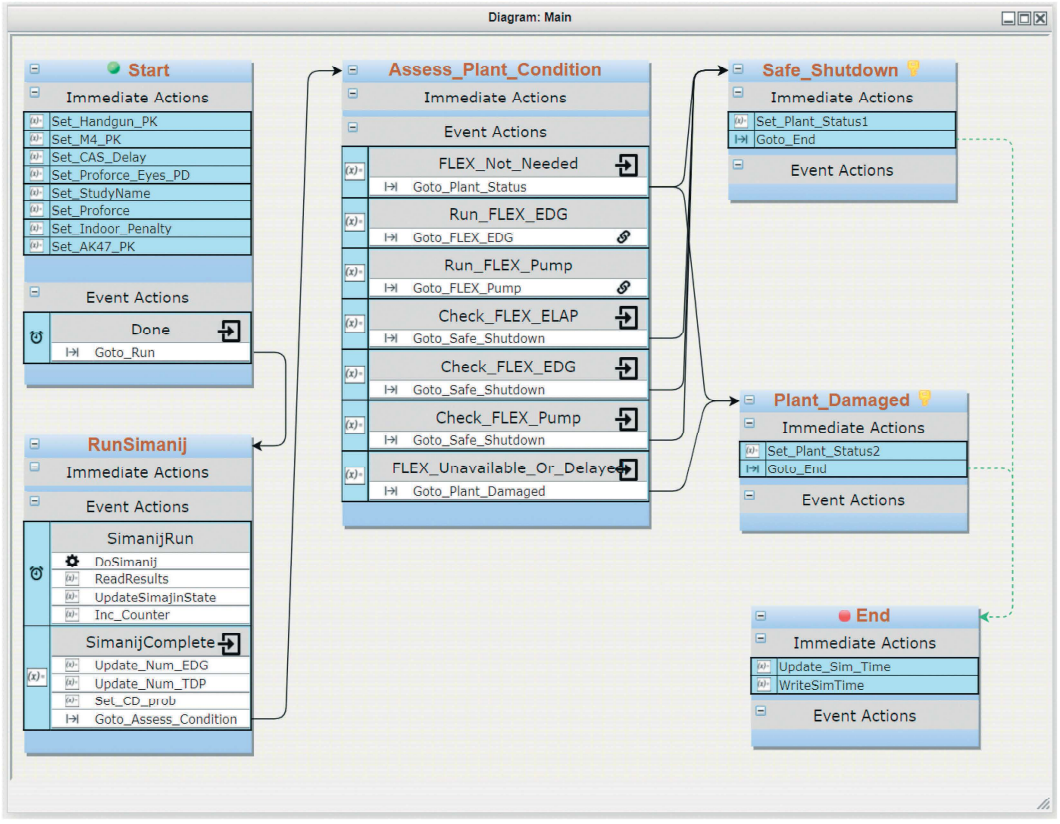


Fig. 10. Main EMRALD diagram.

TABLE III

FLEX Procedure

Number	Steps	Notes
1	Get keys and open doors.	Preparation
2	Assess condition of plant system and equipment.	Execution
3	Contact strategic alliance for FLEX emergency response control center to inform the ELAP event.	Execution
4	Connect FLEX steam generator makeup pump's hose.	Preparation
5	Establish configuration to support FLEX 480-V ac installation.	Execution
6	Connect FLEX cables to 480-V MCCs.	Preparation
7	Open all breakers on MCCs.	Execution
8	Connect FLEX RCS[a] makeup pump hoses.	Preparation
9	Inform security of security area access breaches.	Execution
10	Put a FLEX diesel in service.	Preparation
11	Restore partial lighting and receptacle power.	Execution
12	Turn on supply breaker in FLEX DG enclosure.	Preparation
13	Evaluate potential usages for the portable equipment being delivered from the RRC[b].	Execution
14	Ensure support equipment is staged.	Preparation
15	Establish communications.	Execution

[a]RCS = Reactor Coolant System.
[b]RCS = Reactor Coolant System.

connected, the simulation continues to the *FLEX_DG_On* state. If the FLEX generator fails to run, the operator attempts to repair it, which is modeled in the *FLEX_DG_Status* state. The time to perform this repair is randomly sampled from a normal distribution. It is assumed there is a 0.8 probability to repair the generator.

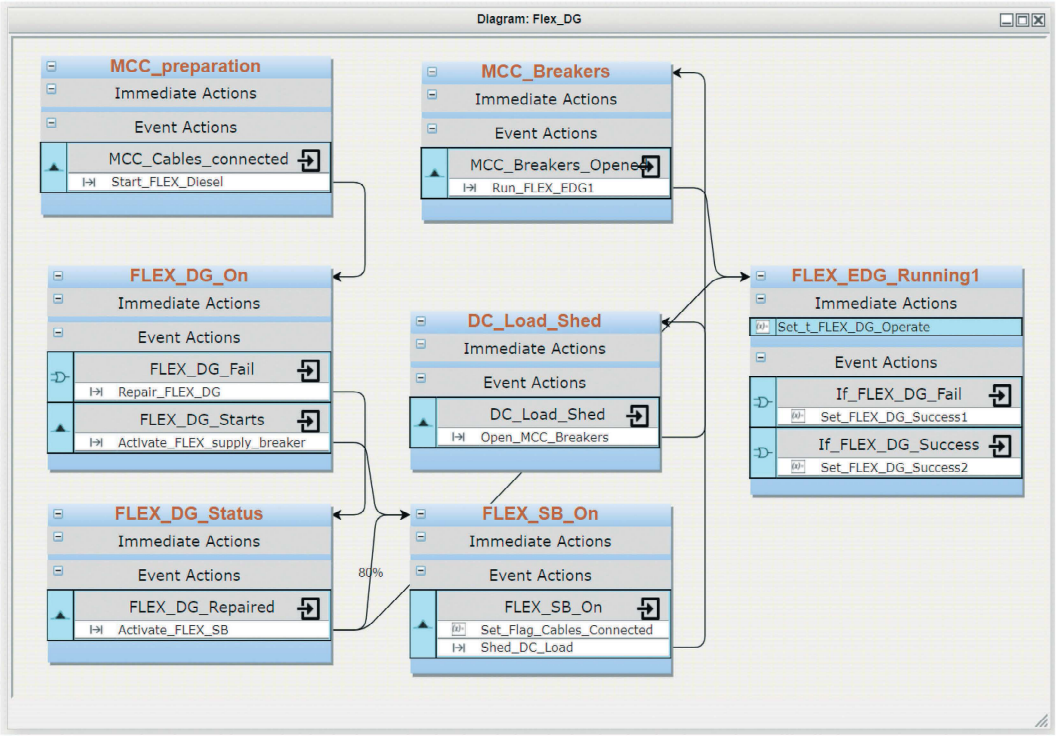


Fig. 11. EMRALD diagram for FLEX DG strategy.

After the generator run, the supply breaker is turned on, a direct-current load shed is performed, and the MCC breakers are opened. The time required to perform all these actions is added to the mobilization time from the FOF simulation and recorded as *t_FLEX_DG_Operate* in the *FLEX_EDG_Running1* state.

If the coolant circulation capability is lost, the FLEX pump strategy is initiated. As shown in Fig. 12, this strategy begins with connecting hoses between the FLEX pump and the coolant inlet ports. After the hoses are connected, the operator aligns the FLEX pump and the transfer switch. The timing for each of these actions is randomly sampled from normal distributions. The cumulative time required to perform these actions is summed with the mobilization time from the FOF simulation and recorded as *t_FLEX_Pump_Operate* in the *FLEX_Pump_Running* state.

The operational states of the FLEX generator are modeled in EMRALD as shown in Fig. 13. The *FLEX_DG1_Standby* state runs when the simulation starts. When a demand for the FLEX generator comes (i.e., when the simulation enters the *FLEX_DG_On* state in Fig. 11), the *FLEX_DG1_Demand* event initiates. It is assumed the generator has a 3E−2 probability of failing to start. If it starts successfully, the *FLEX_DG1_Active* state is initiated. The *FLEX_DG1_FR* is an event based on the specified failure rate of the generator. When the generator fails—either fails to start or fails to run—for 24 h, the *FLEX_DG1_Fail* state is initiated. If the operator manages to repair it (i.e., when the simulation enters the *FLEX_SB_On* state in Fig. 11), the *FLEX_DG1_Repaired* event is activated, and the generator returns to its operational state.

Figure 14 shows the diagrams for the FLEX pump's states. When demand comes (i.e., when EMRALD enters the *FLEX_Pump_Running* state in Fig. 12), the *FLEX_AFW_P1_Demand* event is activated. This event starts the pump with a 0.97 success probability. If the pump fails to start or fails to run, it remains in the failed state until the simulation ends.

III. RESULTS AND DISCUSSION

Multiple runs of simulations for each attack scenario are needed to obtain the probabilistic risk from that scenario. It is necessary to ensure a sufficient number of simulations are performed to provide a reliable estimate of the probability value. Therefore, a convergence analysis was conducted to determine the minimum number of runs needed for reliable conditional core damage probability (CCDP) values. The results are shown in Figs. 15 through 18 for the attack scenarios A through D,

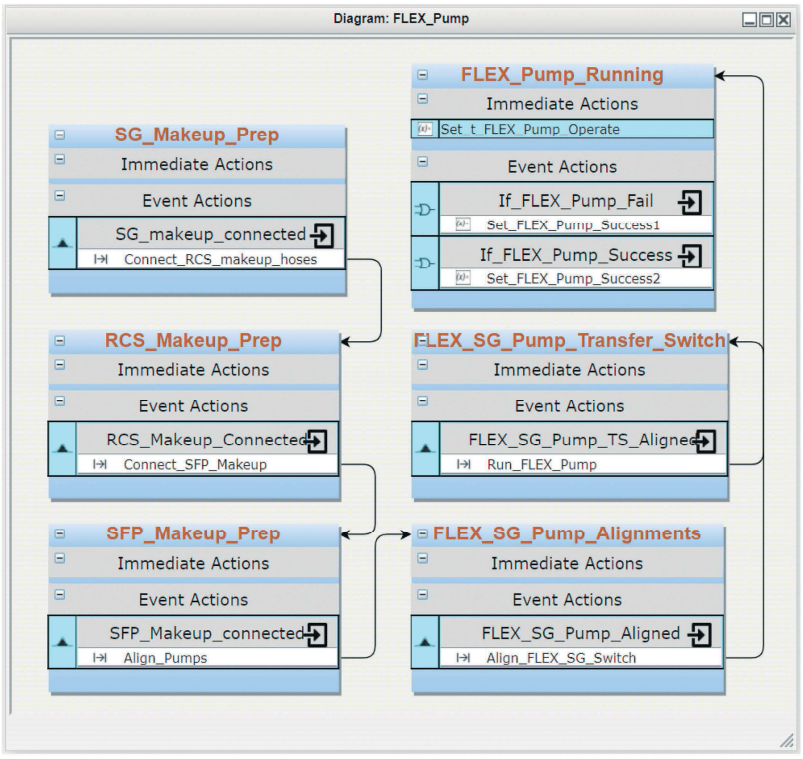


Fig. 12. EMRALD diagram for the FLEX pump strategy.

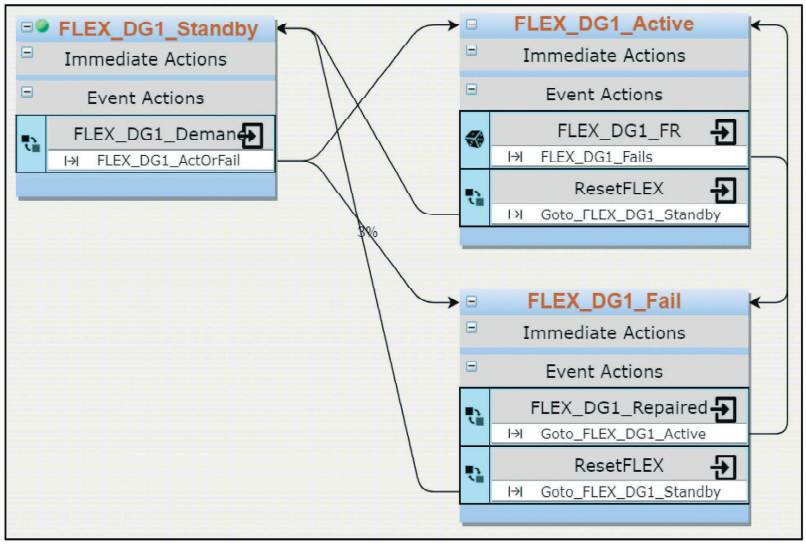


Fig. 13. Diagram of FLEX generator's operational states.

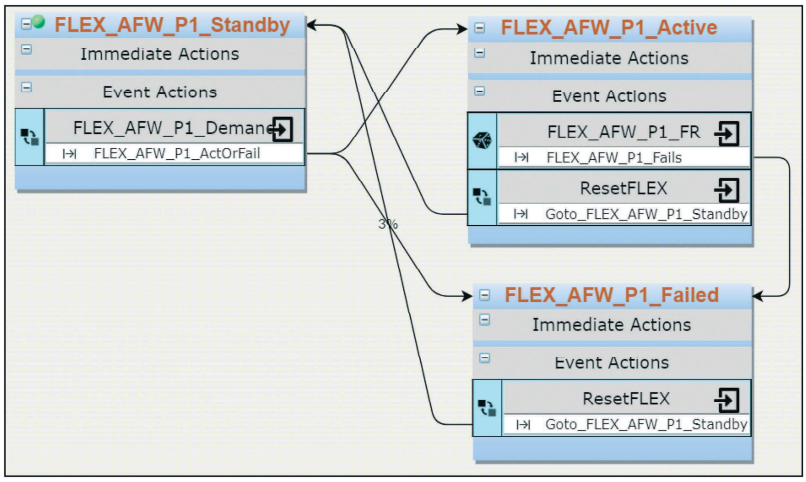


Fig. 14. Diagram of FLEX pump's operational states.

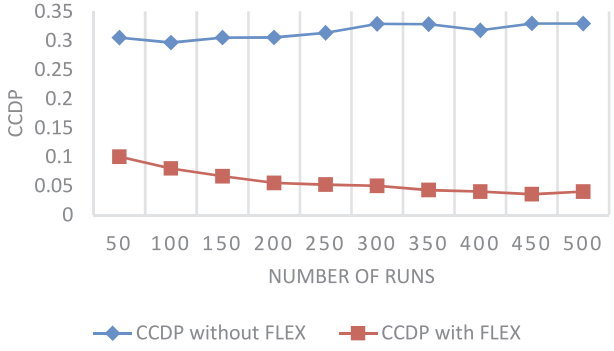


Fig. 15. Convergence analysis for attack scenario A.

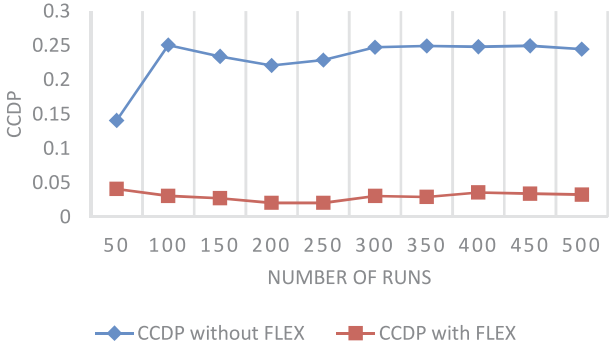


Fig. 16. Convergence analysis for attack scenario B.

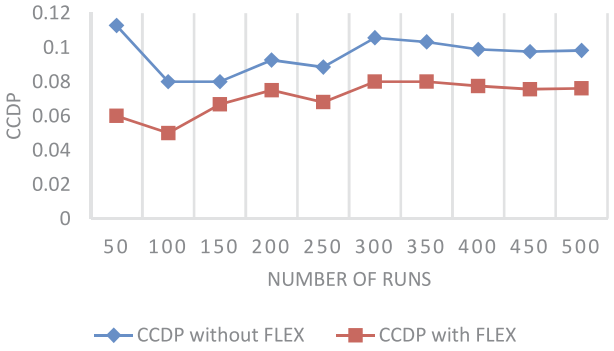


Fig. 17. Convergence analysis for attack scenario C.

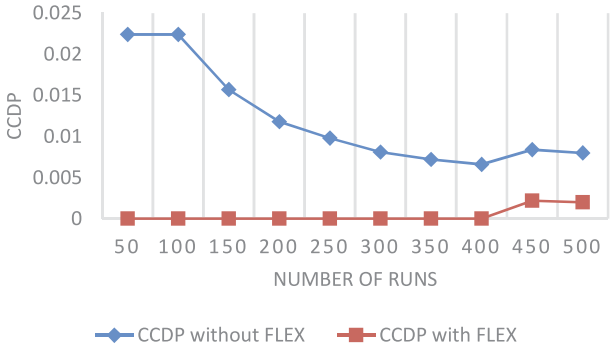


Fig. 18. Convergence analysis for attack scenario D.

respectively. The results show the probability metric starts to stabilize from 400 simulation runs. Based on this observation and considering the fact FOF simulations are computationally expensive, it was decided to run the simulation for 500 runs per scenario.

The integrated FOF-FLEX model was simulated with the initial attackers. A total of 500 simulations were run for each of the four attack scenarios. Results for the first attack scenario (scenario A) are summarized in Table IV. The FOF probability is the number of observed events divided by the total simulation runs of 500. The CCDP is the product of the FOF probability with the CD probability if the respective event happens. The CD probabilities when the FLEX strategy is not used may be taken from plant-specific PRA models. However, these values are reasonably assumed for the hypothetical plant used in this study. Meanwhile, the CD probabilities with the FLEX strategy are computed from the EMRALD simulation when FLEX equipment fails to operate or is operated beyond the conservative time limit of 1 h. Some of the attack outcomes in Table IV did not occur

TABLE IV

CCDP Calculations for Attack Scenario A with Initial Base Model

Scenario Number	Availability				Number of Events from FOF Simulation	Scenario Probability	CCDP Without FLEX	CCDP with FLEX
	EDG[a]	TDP	FLEX DG	FLEX Pump				
1	Y	Y	Y	Y	384	7.68E−1	7.68E−1 × 1E−3	7.68E−1 × 2E−4
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	7.2E−2	7.2E−2 × 1	7.2E−2 × 0.2
10	N	Y	Y	N	0	0	0 × 1	0 × 0.2
11	N	Y	N	Y	0	0	0	0
12	N	Y	N	N	0	0	0	0
13	N	N	Y	Y	77	1.54E−1	1.54E−1 × 1	1.54E−1 × 0.2
14	N	N	Y	N	0	0	0 × 1	0 × 1
15	N	N	N	Y	2	4E−3	4E−3 × 1	4E−3 × 1
16	N	N	N	N	1	2E−3	2E−3 × 1	2E−3 × 1
Total					500	1	2.33E−1	5.14E−2

[a]Y = Yes, N = No.

TABLE V

Overall Failure Probabilities of the DBT Attack Scenarios

Scenario	Importance Measure		Weight-Adjusted CCDP	
	Without FLEX Strategy	With FLEX Strategy	Without FLEX Strategy	With FLEX Strategy
Scenario A	91.73%	81.41%	2.14E−1	2.07E−2
Scenario B	5.12%	13.46%	6.66E−4	5.65E−4
Scenario C	1.18%	1.92%	3.55E−5	1.15E−5
Scenario D	1.97%	3.21%	9.85E−5	3.21E−5
Total	100.00%	100.00%	2.14E−1	2.13E−2

TABLE VI

Base and DID Models

	Scenario A	Scenario B	Scenario C	Scenario D
Base model	Alpha team of three adversaries and Bravo team of three adversaries	Alpha team of three adversaries and Bravo team of three adversaries	Alpha team of three adversaries and Bravo team of three adversaries	Alpha team of three adversaries and Bravo team of three adversaries
DID model	Alpha team of six adversaries and Bravo team of six adversaries	Alpha team of six adversaries and Bravo team of six adversaries	Alpha team of six adversaries, Bravo team of six adversaries, Charlie team of one adversary providing over-watch support	Alpha team of six adversaries, Bravo team of six adversaries, Charlie and Delta team each of one adversary providing over-watch support

TABLE VII

CCDP Calculations for the First Attack Scenario with Beyond-DBT Adversaries

Number	System Availability				Number of Events	FOF Probability	CCDP Without FLEX	CCDP with FLEX
	EDG[a]	TDP	FLEX DG	FLEX Pump				
1	Y	Y	Y	Y	276	0.552	0.552 × 1E−3	0.552 × 2E−4
2 through 8	Y	*	*	*	0	0	0	0
9	N	Y	Y	Y	62	0.124	0.124 × 1	0.124 × 0.2
10, 11, and 12	N	Y	*	*	0	0	0	0
13	N	N	Y	Y	142	0.284	0.284 × 1	0.284 × 0.2
14	N	N	Y	N	3	6E−3	6E−3	6E−3
15	N	N	N	Y	13	2.6E−2	2.6E−2	2.6E−2
16	N	N	N	N	4	8E−3	8E−3	8E−3
Total					500	1	0.4485	0.1217

[a]Y = Yes, N = No.

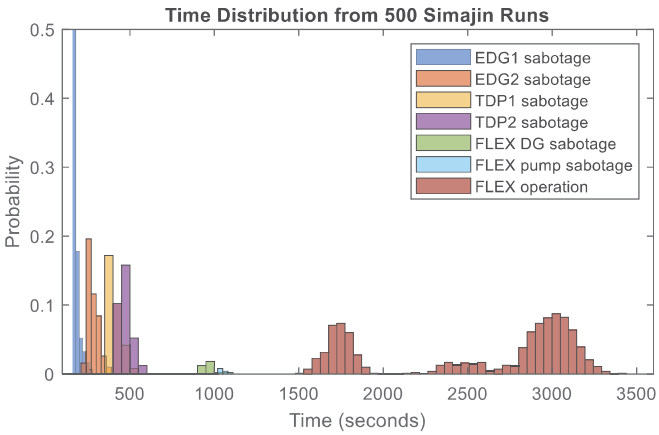


Fig. 19. Time distribution of events in scenario A.

backup equipment to mitigate the adverse effects of security incidents. This margin can be leveraged to optimize the PPS, particularly the number of armed responders.

The DID models were investigated to analyze the physical security effectiveness beyond the outermost layer of protection. For this demonstration, the DID scenarios were simulated by increasing the number and attack capabilities of the adversary team. Details of the selected base and DID models are given in Table VI, following our previous publication.[23]

Results for the first scenario of the DID model are given in Table VII. The outcomes with zero probabilities are collapsed to highlight the more significant data.

TABLE VIII

Overall Adversary Success Probability of Beyond-DBT Attack Scenarios

Scenario	Importance Measure		CCDP	
	Without FLEX Strategy	With FLEX Strategy	Without FLEX Strategy	With FLEX Strategy
Scenario A	45.37%	27.8%	2.03E−1	3.38E−2
Scenario B	27.96%	22.14%	7.73E−2	2.15E−2
Scenario C	9.19%	18.05%	8.36E−3	1.43E−2
Scenario D	17.48%	32.01%	3.02E−2	4.48E−2
Total	100.00%	100.00%	2.93E−1	1.1E−1

because the adversaries were assumed to strike target components in succession. For example, if adversaries have not sabotaged the first component in their target list, they will not skip it to attack the second component.

Several assumptions were made for Table IV. The CCDP without FLEX is set to 1E−3 following NUREG/CR-6890 (Ref. 21). The FLEX failure probability is assumed to be 0.2. This is a rough approximation of the FLEX equipment fail-to-run and fail-to-start probabilities for a 24-h mission time period based on a technical reference document.[22] FLEX equipment is assumed to be used as a backup in case the design-basis safety system fails. Therefore, the CCDP with FLEX is 2E−4.

Table IV shows that using the FLEX mitigation strategy reduces the adversary success probability for this attack scenario. However, this result is for only one attack scenario. Results for the whole scenario set are summarized in Table V. This table shows that the use of the FLEX strategy reduces the overall adversary success probability by an order of magnitude. It illustrates the probability margin obtained from utilizing Comparing Tables IV and VII demonstrates that adversaries are more likely to penetrate through the PPS and damage the targets with an increased attack capability. A higher probability of an adversaries' success increased the FOF probabilities for outcome numbers 9 through 16, which in turn increased the CCDP values.

Figure 19 visualizes the event timing in scenario A. This includes the time histogram of sabotage events and the operation of FLEX equipment. Operators start to initiate a FLEX procedure when the respective safety function from the design-basis equipment is lost. Because the adversaries sabotage TDP pumps later than the DGs, the histogram of the FLEX operation has two distinct peaks corresponding to the timing when the safety functions of the DGs and TDP pumps are lost.

The methodology shown in Table VII is repeated for the other attack scenarios. Results are summarized in Table VIII. As expected, the beyond-DBT attacks increased the CCDP for each attack scenario.

Each post's effectiveness in neutralizing adversaries is calculated using Eqs. (6) and (7). The results for the first

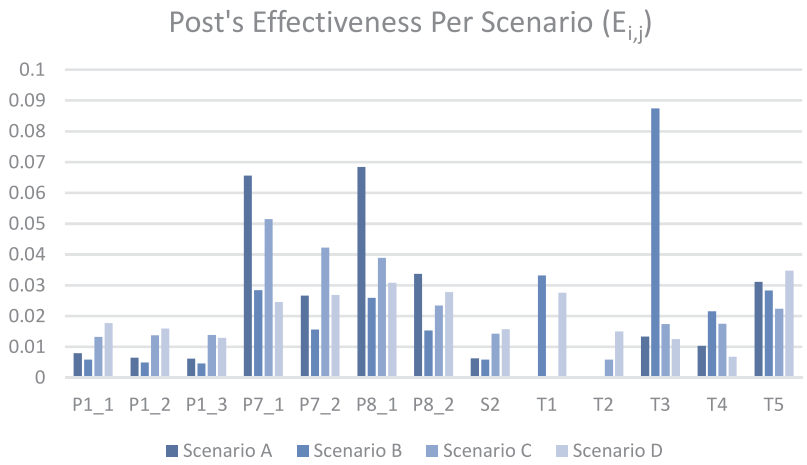


Fig. 20. Post's effectiveness per scenario for the first iteration.

iteration are shown in Fig. 20 by removing noncombatant posts. The figure shows how effective a post is in neutralizing adversaries for each attack scenario. Figure 21 shows the total effectiveness for each post calculated with Eq. (8), highlighting T2 as the least effective post.

After removing T2 from the FOF model, the simulation is iterated again. With fewer posts, the PPS is less effective. However, the margin due to the use of the FLEX mitigation strategy can be recovered to compensate for the reduction in the number of posts. The least effective post is identified and removed from the model as long as the adversary success probability is less than the adversary success probability without FLEX. Through the iterative process of determining the least effective posts, it is found that four posts can be excluded from the response force while still maintaining the adversary success probability below the initial adversary success probability. The adversary success probability and remaining margin in each iteration is displayed in Fig. 22. It shows that the adversary success probability when five posts are removed exceeds the initial adversary success probability; therefore, that configuration is not selected.

The methodology of security optimization in this study is deemed conservative because it elevates the adversary's capabilities. This approach is selected to evaluate the PPS DID elements without running many computationally expensive FOF simulations. The optimized PPS is then validated using the initial attack capability to verify that it does not increase the adversary success probability relative to the initial PPS configuration. The result of this verification is shown in

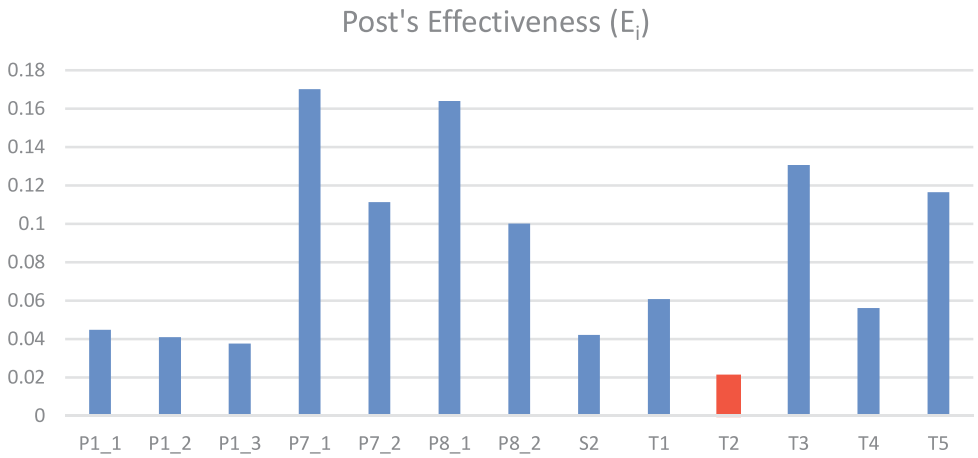


Fig. 21. Post's total effectiveness for the first iteration.

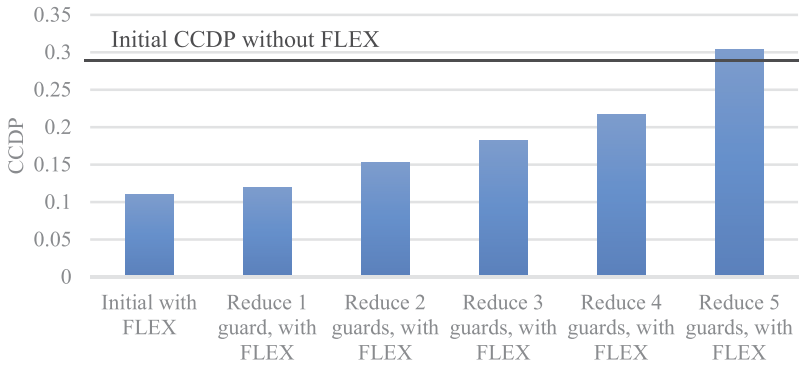


Fig. 22. Adversary success probability and margin for the DID models.

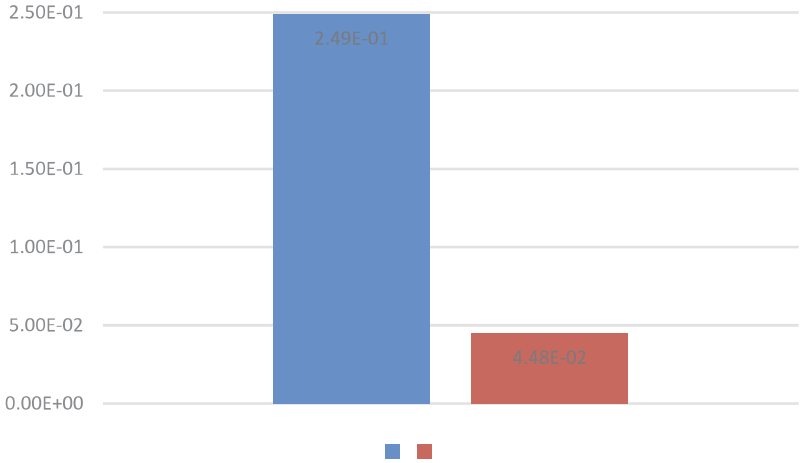


Fig. 23. Adversary success probability comparison for the DBT attacks.

Fig. 23. 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.

IV. CONCLUSION

This paper provides an overview of a methodology for integrating FOF simulation tools and a dynamic risk simulation tool (EMRALD) to evaluate and optimize the physical security effectiveness for a NPP. The proposed methodology could be used to evaluate the effectiveness of various potential physical security enhancements and to provide an understanding of the corresponding reduction in the number of armed responders that could potentially be realized by implementing a new strategy that still provides equivalent protection of the facility. One example presented in this paper would be for the inclusion of FLEX equipment into the plant protection strategy.

Using a generic plant model of a hypothetical facility, the initial analysis indicates a likely significant reduction in the overall risk of CD due to sabotage of the plant if FLEX equipment is considered in the overall mitigation strategy. The additional safety margin that is observed by crediting FLEX equipment could then be analyzed to support the justification to a modification of the facility's physical protection posture that provides an equivalent or higher level of protection with fewer armed responders. This paper provides an overview of the methodology, specific metrics for evaluating effectiveness, and a process to evaluate potential savings that could be realized through implementation of the revised physical protection strategy. Since this initial analysis was conducted using a generic model and hypothetical facility, additional work is required to demonstrate the usability and applicability for an actual facility.

Disclosure Statement

No potential conflict of interest was reported by the authors.

References

1. J. ZAMANALI, C. CHWASZ, and J. E. VAUGHN, "Nuclear Power Plant Security Assessment Guide," NUREG/CR-7145, Nuclear Regulatory Commission (Apr. 2013); https://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr7145/index.html (current as of Mar. 30, 2022).
2. D. W. WHITEHEAD, C. S. POTTER, and S. L. O'CONNOR, "Nuclear Power Plant Security Assessment Technical Manual," SAND2007-5591, Sandia National Laboratories (Sep. 2007).
3. *Code of Federal Regulations*, Title 10, Part 73, Section 1, "General Provisions," U.S. Nuclear Regulatory Commission; https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0001.html (current as of Mar. 30, 2022).
4. "Guidance for the Application of the Radiological Sabotage Design Basis Threat in the Design, Development, and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements (SGI)," Regulatory Guide 5.69, Rev. 1, U.S. Nuclear Regulatory Commission (Mar. 2022).
5. "Nuclear Power Plants Security Assessment Standard Set of Scenarios," U.S. Nuclear Regulatory Commission (Dec. 2007).
6. "Regulatory Guide 5.81, Rev. 1, 'Target Set Identification and Development for Nuclear Power Reactors,'" U.S. Nuclear Regulatory Commission (Dec. 2019).
7. Y. A. SETIAWAN, "Adversary Path Analysis of a Physical Protection System Design Using a Stochastic Approach," MS Thesis, Texas A & M University, Department of Nuclear Engineering (May 2018); https://hdl.handl.net/1969.1/173597 (current as of Mar. 30, 2022).
8. R. CHRISTIAN et al., "Methodology and Application of Physical Security Effectiveness Based on Dynamic Force-on-Force Modeling," INL/EXT-20-59891, Idaho National Laboratory (Sep. 2020); https://lwrs.inl.gov/Physical%20Security/Methodology_Application_Physical_Effectiveness_based_on_FoF.pdf (current as of Mar. 30, 2022).
9. "Diverse and Flexible Coping Strategies (FLEX) Implementation Guide," NEI 12-06, Nuclear Energy Institute (Aug. 2012); https://www.nrc.gov/docs/ML1222/ML12221A205.pdf (current as of Mar. 30, 2022).
10. "Physical Protection Programs at Nuclear Power Reactors," 85 FR 76625, U.S. Nuclear Regulatory Commission (Nov. 2020).
11. R. CHRISTIAN et al., "Methodology and Application of Physical Security Effectiveness Based on Dynamic Force-on-Force Modeling," presented at the 2021 Int. Topl. Mtg. on Probabilistic Safety Assessment and Analysis (PSA 2021), Columbus, Ohio.
12. M. L. GARCIA, *Design and Evaluation of Physical Protection Systems*, 2nd ed., Butterworth-Heinemann, Burlington, Massachusetts (2007).
13. I. C. E. WELY and A. CHETAINE, "Analysis of Physical Protection System Effectiveness of Nuclear Power Plants Based on Performance Approach," *Ann. Nucl. Energy*, **152**, 107980 (2021); https://doi.org/10.1016/j.anucene.2020.107980.
14. A. A. WADOUD, A. S. ADAIL, and A. A. SALEH, "Physical Protection Evaluation Process for Nuclear Facility via Sabotage Scenarios," *Alexandria Eng. J.*, **57**, *2*, 831 (2018); https://doi.org/10.1016/j.aej.2017.01.045.
15. B. ZOU, M. LI, and M. YANG, "Vulnerability Learning of Adversary Paths in Physical Protection Systems Using AMC/EASI," *Prog. Nucl. Energy*, **134**, 103666 (2021); https://doi.org/10.1016/j.pnucene.2021.103666.
16. Y. A. SETIAWAN, S. S. CHIRAYATH, and E. D. KITCHER, "MAPPS: A Stochastic Computational Tool for Multi-Path Analysis of Physical Protection Systems," *Ann. Nucl. Energy*, **137**, 107074 (2020); https://doi.org/10.1016/j.anucene.2019.107074.
17. B. ZOU et al., "Evaluation of Vulnerable Path: Using Heuristic Path-Finding Algorithm in Physical Protection System of Nuclear Power Plant," *Int. J. Crit. Infrastruct. Prot.*, **23**, 90 (2018); https://doi.org/10.1016/j.ijcip.2018.08.006.
18. M. H. SILVA et al., "Using Virtual Reality to Support the Physical Security of Nuclear Facilities," *Prog. Nucl. Energy*, **78**, 19 (2015); https://doi.org/10.1016/j.pnucene.2014.07.004.
19. J. CONWAY et al., "Physical Security Analysis and Simulation of the Multi-Layer Security System for the Offshore Nuclear Plant (ONP)," *Nucl. Eng. Des.*, **352**, 110160 (2019); https://doi.org/10.1016/j.nucengdes.2019.110160.
20. D. KANG and S. CHANG, "The Safety Assessment of OPR-1000 Nuclear Power Plant for Station Blackout Accident Applying the Combined Deterministic and Probabilistic Procedure," *Nucl. Eng. Des.*, **275**, 142 (2014); https://doi.org/10.1016/j.nucengdes.2014.05.009.
21. "Reevaluation of Station Blackout Risk at Nuclear Power Plants," NUREG/CR-6890, Vol. 2, U.S. Nuclear Regulatory Commission (Dec. 2005).
22. "FLEX Equipment Data Collection and Analysis," PWROG-18043-P Rev. 0, Pressurized Water Reactor Owners Group (Feb. 2020).
23. R. CHRISTIAN et al., "Integration of Physical Security Simulation Software Applications in a Dynamic Risk Framework," Idaho National Laboratory (Aug. 2021).