INL/EXT-21-64333
Revision 0

Light Water Reactor Sustainability Program

Integration of Physical Security Simulation Software Applications in a Dynamic Risk Framework

August 2021

U.S. Department of Energy

Office of Nuclear Energy

INL/EXT-21-64333
Revision 0

Integration of Physical Security Simulation Software Applications in a Dynamic Risk Framework

Robby Christian
Steven R. Prescott
Vaibhav Yadav
Shawn W. St Germain
Christopher P. Chwasz

August 2021

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

SUMMARY

The overall operation and maintenance cost to protect nuclear power plants accounts for approximately 7% of power generation's total cost with labor accounting for half of this cost. In the current research, from interactions with utilities and other stakeholders, it was determined physical security forces account for nearly 20% of the entire workforce at several nuclear power plants. Labor costs continue to rise in the U.S., so any measures to reduce the cost of operating a nuclear power plant will need to include a reduction in labor. The physical security pathway within the Department of Energy's Light Water Reactor Sustainability program aims to lower the cost of physical security through directed research into modeling and simulation, application of advanced sensors, or deployment of advanced weapons.

This report describes the research and development being performed at Idaho National Laboratory toward a dynamic modeling and simulation framework to enable physical security optimization at commercial nuclear power plants. The framework is based on Event Modeling Risk Assessment using Linked Diagrams (EMRALD), the dynamic modeling tool, and is demonstrated for applications that can result in physical security optimization. Two main applications are presented: (1) physical security optimization by staff reduction analysis and (2) extension of the existing force-on-force and diverse and flexible mitigation capability (FLEX) integration framework across (a) another commercially available force-on-force tool and (b) a comprehensive set of attack scenarios.

The presented analysis is focused on optimizing physical security posture at nuclear power plants by performing a reduction in the number of armed guards. The optimization framework starts with evaluating the effectiveness of the current physical security posture and is followed by a defense-in-depth analysis and staff reduction evaluation. The staff reduction evaluation analysis entails an iterative framework that identifies the least effective post in the plant physical security posture across an extensive set of potential attack scenarios. The framework then recommends removal of the least effective post only if the removal has minimal impact on the performance effectiveness of the overall security posture.

The INL's existing framework for modeling FLEX portable equipment is extended to integrate with force-on-force modeling in another popular commercial tool, Simajin. This report presents several case studies of modeling adversarial attacks aimed at causing a radiological release by sabotaging the plant's critical assets at a hypothetical pressurized-water reactor. The results

demonstrate even in the extreme case of a successful adversarial attack, deploying FLEX equipment can result in a significantly high likelihood of preventing radiological release. The modeling and simulation framework of integrating FLEX equipment with force-on-force models enables the nuclear power plants to credit FLEX portable equipment in the plant security posture resulting in an efficient and optimized physical security. The presented work has resulted in integrating Idaho National Laboratory's dynamic simulation tool, EMRALD, with three force-on-force simulation tools, SCRIBE3D, AVERT, and Simajin, of which the latter two are currently being used by a majority of commercial nuclear power plants across the nation for their force-on-force modeling. Integrating EMRALD with these tools paves way for wide implementation of Idaho National Laboratory's physical security optimization framework at commercial nuclear power plants.

NOTE: The work performed in this report leverages an existing hypothetical example used for domestic and international physical security training, the Lone Pine nuclear power plant facility, for target sets and modeling. The information used for the design basis threat (DBT) is also hypothetical and not based on any performance testing. The results are displayed as an example of a process only and do not represent any actual facility or adversary capability.

CONTENTS

SUMMARY iii

ACRONYMS vii

1. INTRODUCTION 1

2. PHYSICAL SECURITY OPTIMIZATION 2
   - 2.1 Base Case Evaluation 2
     - 2.1.1 Scenario Sets 3
     - 2.1.2 PPS Effectiveness and Comparison Calculation 3
     - 2.1.3 Defense-in-Depth Analysis 5
   - 2.2 Potential Strategy Evaluation 6
   - 2.3 Staff Reduction Evaluation 8
     - 2.3.1 Evaluating Least Effective Post 9
     - 2.3.2 Running the Modified Strategy Model 10
     - 2.3.3 Compare with DID Base Case 10
     - 2.3.4 Apply and Verify 10

3. FOF-FLEX INTEGRATION 11
   - 3.1 Case Study 12
     - 3.1.1 Scenario Description 12
     - 3.1.2 FLEX Implementation in EMRALD 14
   - 3.2 Results and Discussion 20
     - 3.2.1 Convergence Analysis 20
     - 3.2.2 Probability Calculation 22
     - 3.2.3 Evaluating Least Effective Post 26

4. CONCLUSION AND FUTURE WORK 28

5. REFERENCES 29

Appendix A Description of Attack Scenarios 31

Appendix B EMRALD Model 38

Appendix C Detailed Results 43

FIGURES

Figure 1. Flow for creating base case comparison results. 3

Figure 2. Flow for option evaluation. 7

Figure 3. Process to evaluate staff reduction for a strategy change. 9

Figure 4. FOF-FLEX integration framework. 12

Figure 5. Sabotage scenario to inflict CD. 12

Figure 6. Facility layout and the attack plan in the FOF model. 13

Figure 7. Main EMRALD diagram. 15
Figure 8. EMRALD diagram for FLEX generators. 17
Figure 13. Convergence analysis for the attack Scenario A. 20
Figure 14. Convergence analysis for the attack Scenario B. 21
Figure 15. Convergence analysis for the attack Scenario C. 21
Figure 16. Convergence analysis for the attack Scenario D. 22
Figure 17. Time distribution of events in Scenario A. 25
Figure 18. Ranks of adversary neutralization across attack scenarios. 26
Figure 19. Adversary success probability and margin. 27
Figure 20. Adversary success probability comparison for DBT attacks. 27
Figure A-1. Attack Scenario A. 33
Figure A-2. Attack Scenario B. 34
Figure A-3. Attack Scenario C. 35
Figure A-4. Attack Scenario D. 36
Figure B-1. *DoSimanij* action. 40
Figure B-2. *ReadResults* action. 41

TABLES

Table 1. Example base case (1a) and example change case (1b). 4
Table 2. Original scenarios and DID modified scenario values. 6
Table 3. Original scenarios and DID modified scenario values with an abnormal scenario. 6
Table 4. Combining post statistical data with scenario probabilities and importance. 10
Table 5. Possible attack outcomes. 14
Table 6. FLEX procedure. 16
Table 7. CCDP calculations for the first attack scenario with DBT adversaries. 23
Table 8. Overall failure probabilities of the DBT attack scenarios. 24
Table 9. CCDP calculations for the first attack scenario with beyond-DBT adversaries. 24
Table 10. Overall adversary success probability of beyond-DBT attack scenarios. 25

ACRONYMS

CCDP	conditional core damage probability
CD	core damage
DBT	Design Basis Threat
DG	diesel generators
DID	defense-in-depth
EDG	emergency diesel generator
ELAP	extended loss-of-ac-power
EMRALD	Event Modeling Risk Assessment using Linked Diagrams
FLEX	Diverse and Flexible Mitigation Capability
FOF	force-on-force
IDS	intrusion detection system
INL	Idaho National Laboratory
LOOP	loss-of-offsite-power
LWRS	Light Water Reactor Sustainability
MCC	motor control center
MCUB	minimum cut set upper bound
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
O&M	operation and management
PK	Probability of kill
PPS	physical protection system
PRA	probabilistic risk assessment
PWR	pressurized-water reactor
SAFER	strategic alliance for FLEX emergency response
SAPHIRE	Systems Analysis Programs for Hands-On Integrated Reliability Evaluations
SBO	station blackout
SG	steam generator
TDP	turbine driven pump

Page intentionally left blank

INTEGRATION OF FLEX EQUIPMENT AND OPERATOR ACTIONS IN PLANT FORCE-ON-FORCE MODELS WITH DYNAMIC RISK ASSESSMENT

1. INTRODUCTION

The overall operation and management (O&M) costs to operate a nuclear power plant (NPP) in the U.S. have increased to a point that many utilities may not be able to continue to operate these important assets. The continued low cost of natural gas and the added generation of increased wind and solar development in many markets has significantly lowered the price utilities charge for electricity. Utilities are working hard to modernize plant operations to lower the cost of generating electricity with nuclear power. The Department of Energy established the Light Water Reactor Sustainability Program (LWRS) with the mission to support the current fleet of NPPs with research to facilitate lowered O&M costs. Due to the use of nuclear materials, NPPs have an additional cost burden in protecting fuel against theft or sabotage. The overall O&M cost to protect NPPs accounts for approximately 7% of the total cost of power generation, with labor accounting for half of this cost [1]. In the current research, from interaction with utilities and other stakeholders, it was determined physical security forces account for nearly 20% of the entire workforce at several NPPs. Labor costs continue to rise in the U.S., so any measures to reduce the cost of operating a NPP will need to include a reduction in labor.

To support this mission, a new pathway for physical security research was established within the LWRS program. The physical security pathway aims to lower the cost of physical security through directed research into modeling and simulation, application of advanced sensors or deployment of advanced weapons. Modeling and simulation will be used to evaluate the margin inherent in many security postures and to identify ways to maintain overall security effectiveness while lowering costs. Two areas identified for evaluation include taking credit for diverse and flexible mitigation capability (FLEX) equipment and actions taken by operators to minimize the possibility of reactor damage during an attack scenario. FLEX equipment was installed at all U.S. NPPs as a response to the nuclear accident at Fukushima Daiichi in Japan [1]. FLEX equipment is comprised of portable generators, pumps, and equipment to supply reactor cooling in the event installed plant equipment is damaged. While FLEX equipment was installed to support a plant's response to natural hazards, such as flooding or earthquakes, this equipment could also be used to provide reactor cooling in response to equipment damage caused by an attack on the plant. Likewise, there are certain actions plant operators will take when an attack occurs to minimize the chance of core damage (CD). It will take modeling and simulating the reactor core and systems to evaluate the effect these operator actions may have on increasing the coping time of the reactor.

The Nuclear Regulatory Commission (NRC) and industry approach to maintaining effective security at a plant includes various security programs—each with its own individual objectives; when combined, these programs provide a holistic approach to maintaining the effective security of the plant. The requirements document, 10 CFR 73.55(d)(1), states, "The licensee shall establish and maintain a security organization that is designed, staffed, trained, qualified, and equipped to implement the physical protection program in accordance with the requirements of this section" [4]. NRC security requirements for commercial operating nuclear sites increased exponentially following the September 11 terrorist attacks resulting in a significant increase of onsite response force personnel across the nuclear industry [2]. The plant's response force includes the minimum number of armed responders as required in 10 CFR 73, and security officers tasked with assigned duties, such as stationary observation/surveillance posts, foot-patrol, roving vehicle patrols, compensatory posts, and other duties as required [3].

The nuclear industry needs to pursue an optimized plant security posture that considers efficiencies and innovative technologies to help reduce costs while meeting security requirements. Using FLEX

portable equipment in the plant physical security posture has been identified as one area that holds the potential to optimize the security posture and reduce costs. This report describes the modeling and simulating capabilities developed to incorporate the deployment of FLEX with force-on-force (FOF) modeling of a typical physical security posture at a generic light water reactor plant.

There are several different levels of FOF modeling from simple procedures of adversary and defense force tasks and probabilities to full 3D models with artificial intelligence to determine character paths, detection, and combat [5]. The INL's existing framework for modeling FLEX portable equipment is extended to integrate with FOF modeling in another popular commercial software, Simajin [8], and to evaluate what is needed and include FLEX equipment and procedures into the model. Section 2 provides an overview of the modeling and simulation approach developed in this work for physical security optimization, and Section 3 describes integrating FLEX equipment with FOF modeling and simulation and presents a case study, followed by a conclusion in Section 4.

NOTE: The work performed in this report leverages an existing hypothetical example used for domestic and international physical security training, the Lone Pine nuclear power plant facility for target sets and modeling. The information used for the design basis threat (DBT) is also hypothetical and not based on any performance testing. The results are displayed as an example of a process only and do not represent any actual facility or adversary capability.

2. PHYSICAL SECURITY OPTIMIZATION

Physical security simulation software tools, such as Avert, Simajin, Scribe 3D, etc., can be used to model and simulate the physical protection equipment, strategies, and plausible threat scenarios. These tools and models and likely along with other analysis tools can then be used to optimize many aspects of the physical protection system (PPS) for NPPs by evaluating and potentially incorporating additional strategies. This section describes a process for evaluating and optimizing the defense strategy for new technology, design/procedure changes, or how to include other safety measures, such as FLEX. Different FOF modeling tools have varying capabilities, and some may be able to automatically perform more pieces of this process than others. Depending on the change being evaluated, the process may require coupling the FOF tool to additional simulation tools. Detailed in the following sections, this process consists of three main parts: base case evaluation, potential strategy evaluation, and staff optimization evaluation.

2.1 Base Case Evaluation

Licensee changes to the PPS, as described in the applicable site security plans, must follow the requirements outlined in 10 CFR 50.54(p). Changes that do not "reduce the effectiveness" of the security plans would not require prior commission approval under the 10 CFR 50.90 change process and can be considered acceptable by the NRC under certain conditions. However, NRC reviews and evaluates all licensee security plan changes using the 50.54(p) reduction in effectiveness standard against the status of the security plans and PPS before the approved change to guarantee "high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety." The goal of this evaluation is for a licensee to plan changes to the PPS that provide an equal or greater level of protection while reducing costs. For this analysis' purpose, the current form of the PPS and security plans will be considered sufficient and taken as the baseline condition to compare changes. Additionally, considerations for exemptions from NRC regulations—for example, the reduction in number of armed responders from ten as prescribed in 10 CFR 73.55(k)(5)(ii)—are not considered in this methodology.

This section describes the following steps for calculating a baseline value for comparison from a change in protective strategy, as shown in Figure 1:

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

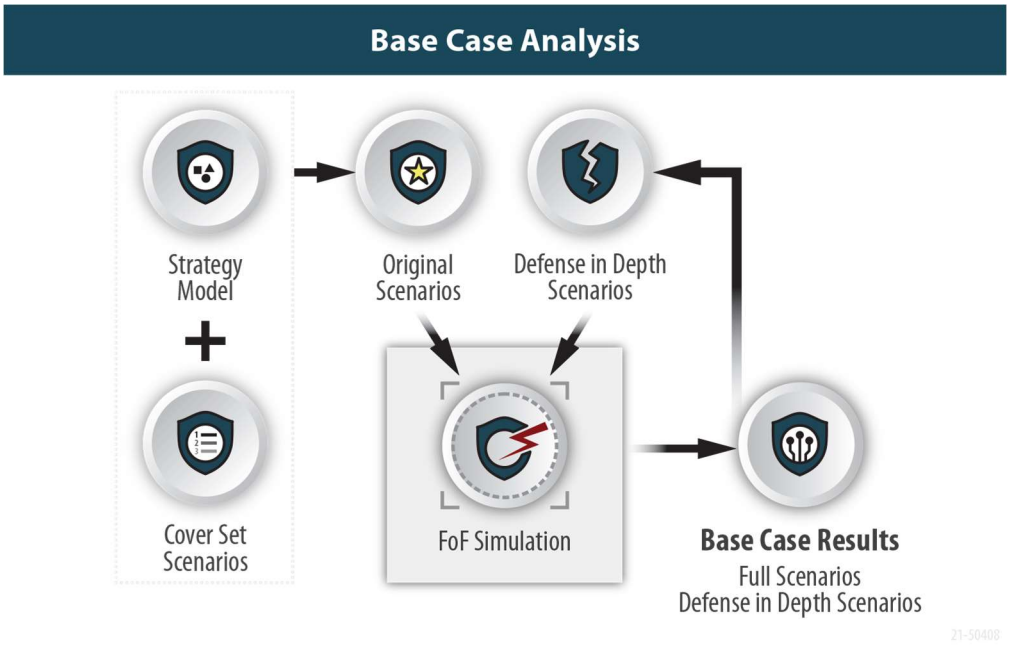


Figure 1. Flow for creating base case comparison results.

2.1.1 Scenario Sets

To demonstrate there is no reduction in PPS effectiveness, a baseline value is developed from a plant's current (presumably sufficient) defensive posture. This is done by modeling in a FOF simulation tool capable of capturing the strategies and procedures established by the NPP. Expert judgement, past FOF exercises, and software tools should be used to identify a cover set of scenarios.

A cover set is a grouping of attack scenarios used for comparing PPS configurations. Cover sets are comprised by one or more target sets (each with one or more adversary pathways) chosen to challenge the proposed change in the physical protection system. Unlike a typical analysis where only the top percentage of scenarios are considered, the cover set must include 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 should be included, and only similar routes with equal or smaller design basis threat (DBT) adversary characteristics should be excluded.

2.1.2 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. We can also frame the effectiveness of the PPS as 1 − PPS success = adversary success, where a lower adversary success denotes a more effective PPS. For this analysis' purpose, we will frame PPS effectiveness in terms of adversary success. A proper PPS analysis will evaluate multiple potential attack scenarios. Evaluating each potential attack scenarios will result in a ranking of scenarios based on the likelihood of the adversary's success.

When changes are made to a PPS, it is possible the probability of adversary success may go down for some scenarios and possibly go up for other scenarios. It is arguable PPS changes that result in increasing the success probability for a scenario starting with a low adversary success probability to anything equal to or below the probability of the previous largest adversary success probability scenario does not significantly decrease the PPS's effectiveness. However, it is also arguable 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 which increased that scenario probability in actuality decreased the PPS's effectiveness against that specific attack path. In the future, statistical weighting system based on the adversary success probability could be used to determine an overall value for comparison, but to keep it simple and to be conservative, a cumulative measure was used for comparing changes in this work. While not the actual probability level, a cumulative process provides a single base case value using a cover set for comparative evaluations, such as the removal of responders, 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 called, "minimum cut set upper bound" (MCUB), was used as it provides a method to equalize the contributing scenarios, so the total never exceeds 100% [12]. As shown by the example on the left side in Table 1a, when using relatively few small probabilities, the sum and MCUB have similar values. However, with more or larger probabilities as shown on the right of Table 1b, the MCUB provides better comparison number. An importance measure should also be calculated for use in determining "least effective post" described in 2.3. This importance measure is the adversary success probability divided by the sum of all the probability scenarios.

Table 1. Example base case (1a) and example change case (1b).

Table 1a: Example Base Case

Scenario	Adversary Success Prob.	Importance Measure
A	0.2	74.91%
B	0.05	18.73%
C	0.01	3.75%
D	0.001	0.37%
E	0.001	0.37%
F	0.001	0.37%
G	0.001	0.37%
H	0.001	0.37%
I	0.001	0.37%
J	0.001	0.37%
	Sum	**Sum**
	0.267	1.0000
	MCUB	
	0.252851026	

Table 1b: Example Change Case

Scenario	Adversary Success Prob.	Importance Measure
A	0.2	12.20%
B	0.2	12.20%
C	0.4	24.39%
D	0.4	24.39%
E	0.2	12.20%
F	0.2	12.20%
G	0.01	0.61%
H	0.01	0.61%
I	0.01	0.61%
J	0.01	0.61%
	Sum	**Sum**
	1.64	1.0000
	MCUB	
	0.858354355	

2.1.3 Defense-in-Depth Analysis

Due to an already high probability of a plant's security being effective, modifying an element of the posture may not result in a significant change in probability of effectiveness and would have a high degree of uncertainty. Therefore, it is desirable to consider an exaggerated data set for DID analysis. In addition to using the probability of effectiveness, one can use other measures collected by FOF simulations, such as the average number of adversaries that make it into a particular security layer. The number of adversaries that get into the vital area or the number of simulations in which the adversary gets into the vital area of an NPP will likely be more sensitive to changes in the defense posture than system effectiveness of the PPS. To fully test the defense strategy and reduce uncertainty, cover sets need to have a significant number of cases with varied pathways, strategies, and targets. If computing resources were unlimited, this could be done by simply increasing the number of simulations runs, but given resource restrictions, it needs be done through a reduction in defense attributes or an increase in adversary characteristics. 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 main purpose is to verify 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 increasing the adversary force beyond the DBT increasing the weapon effectiveness of the adversary, decreasing 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 for reducing the number of responders, as this would remove the responder prematurely and not provide the data needed for evaluating the "least effective post" described in Section 2.3.

While not used for this analysis, an alternate approach in determining system effectiveness that also would account for the sensitivity of changes in the defense posture is to utilize a layer-based approach. The layer-based approach uses a composite technique to compute system effectiveness where scenarios start past the outer protection layers and detection is assumed; each relevant security layer is run in a separate set of simulations. This process requires more model development, but using this approach assures for the defense machinery to come into play when evaluating the posture change and as such provides measures with more granularity than the overall system effectiveness value. When the simpler methods for constructing a DID model fails to test necessary assets, using this method would allow analysts to understand the impact a countermeasure may have on an entire layer and provides a systematic approach to examining security redundancies. If a facility already has a layer-based model, then it is recommended it be used for comparison.

The DID analysis is conducted by applying the modified posture to the base case FOF model, running the simulation using the same cover sets, and observing the change in effectiveness illustrated by the MCUB. The method used to adjust the model may depend on the defense design change; the key is to capture as many failure cases as possible from the simulation while not increasing the adversary advantage enough to eliminate the effect of the change being made. For example, while evaluating the effectiveness of a delay measure, if the number of adversaries is doubled in the DBT so they easily overwhelm original defenses, then an increase in delay may not significantly change the outcome. If the DID model drastically reduces the effectiveness for the modified strategy, it should be verified the modifications have a similar change in effectiveness percentage as a less severe DID model.

When developing the DID model, another concern to watch for is if scenarios that previously had a very low probability of adversary success drastically increase in comparison to the other scenarios. Invalid increases could cause comparisons to be overly conservative in the process described in Section 2.3. By applying the same method to reduce effectiveness to each scenario, the DID model will likely have similar order and importance comparisons as the original results as shown below in Table 2. If a very low probability of adversary success scenario increases drastically in importance as shown below for Scenario F of DID Modification C in Table 3, verify that an appropriate effectiveness reduction process

was applied to the scenario. If it is correct, then this indicates a more vulnerable scenario to DID and will proportionally affect the comparison results as intended.

Table 2. Original scenarios and DID modified scenario values.

Original			DID Modifications B		
Scenario	**Adversary Success Prob.**	**Importance Measure**	**Scenario**	**Adversary Success Prob.**	**Importance Measure**
A	0.011	40.29%	A	0.51	40.48%
B	0.01	36.63%	B	0.53	42.06%
C	0.003	10.99%	C	0.1	7.94%
D	0.0015	5.49%	D	0.04	3.17%
E	0.0015	5.49%	E	0.05	3.97%
F	0.0003	1.10%	F	0.03	2.38%
	Sum	**Sum**		**Sum**	**Sum**
	0.0273	1.0000		1.26	1.0000
	MCUB			**MCUB**	
	0.027045626			0.816640667	

Table 3. Original scenarios and DID modified scenario values with an abnormal scenario.

Original			DID Modifications C		
Scenario	**Adversary Success Prob.**	**Importance Measure**	**Scenario**	**Adversary Success Prob.**	**Importance Measure**
A	0.011	40.29%	A	0.51	33.33%
B	0.01	36.63%	B	0.53	34.64%
C	0.003	10.99%	C	0.1	6.54%
D	0.0015	5.49%	D	0.04	2.61%
E	0.0015	5.49%	E	0.05	3.27%
F	0.0003	1.10%	F	0.3	19.61%
	Sum	**Sum**		**Sum**	**Sum**
	0.0273	1.0000		1.53	1.0000
	MCUB			**MCUB**	
	0.027045626			0.867678832	

The number of failure cases will significantly increase even without a large decrease in effectiveness. For example, in 5,000 simulations, if the base case effectiveness is 98%, only 100 evaluation cases are available, but with a DID model of 91% effectiveness, 450 cases would be generated from the 5,000 simulations. The evaluations corresponding to failure cases will be used to evaluate the modified strategies and can clearly identify improvements or defense reductions where only using the original base case tests would show little to no change.

2.2 Potential Strategy Evaluation

Each facility can have different options they consider when optimizing their defensive posture. Some options can be evaluated in a research setting for a variety of facilities meeting defined conditions. Others

could be site specific, and a potential evaluation should be done to determine the probable and best improvement options before the full in-depth modeling process is done and evaluated, as described in Section 2.1.

The critical part in evaluating a potential change is having a tool that can correctly simulate a response or effect of a potential change and apply those effects to the FOF simulation. If the FOF simulation tool used for the base case evaluations has the capability to model the change correctly or conservatively, this evaluation can be a fairly simple process. Some protection strategies can require complex modeling of operator procedures and timing, such as using the FLEX equipment designed for beyond-design external events as additional safety equipment after an attack. Other strategies may include simple actions but need plant system modeling or thermal dynamics to get more precise failure timing. These would require coupling the FOF simulation with other tools needed to correctly model the plant behavior.

For this initial research, the Idaho National Laboratory (INL) Event Modeling Risk Assessment using Linked Diagrams (EMRALD) tool is coupled with the Simajin [8] FOF simulation tool [7]. EMRALD allows the user to model complex operator actions and couple that model with the FOF simulation by using data from the FOF model to make decisions or adjust the FOF model according to events in the EMRALD model and then use the FOF data to determine the plant status.

Once the change needing an evaluation is modeled, the DID scenarios can be run using that new model. If the results show a significant improvement to the base case DID results, it can move on to the staff reduction evaluation process.

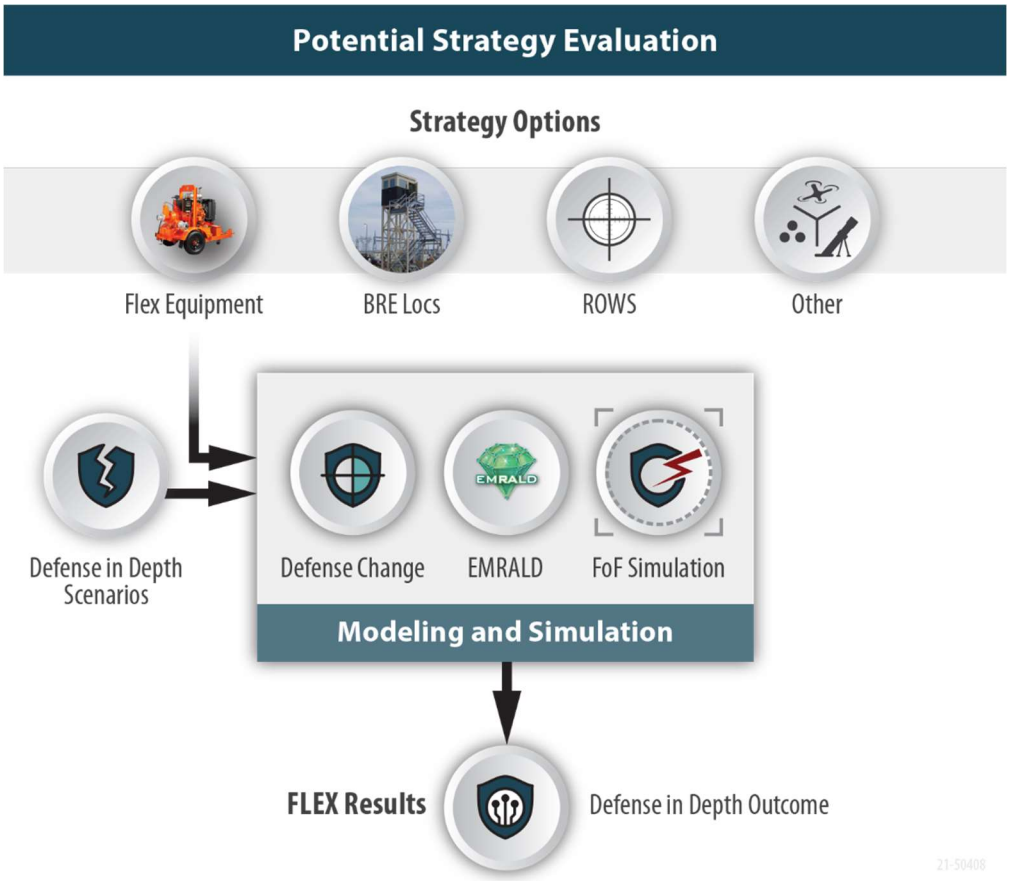


Figure 2. Flow for option evaluation.

In summary, the following steps are used to evaluate a potential strategy protection option, shown in Figure 2:

1. Determine likely improvement methods for strategy change
2. Build a model of those changes using an appropriate tool or tool combination
3. Apply the DID scenarios to the new model/s and run the simulations
4. Compare the results to the original DID results.

2.3 Staff Reduction Evaluation

Once likely improvement methods have been identified and modeled, the process for determining a staffing reduction can begin. This process will ensure an equivalent or better protective strategy efficacy is maintained even after a potential staff reduction. The five main steps to this process are outlined in Figure 3 and described below. Before the process begins, a copy of the original and DID base case cover set and results are generated. This is an iterative process and stops once the criteria has been met. The following summarizes the loop process, and the subsections give details and specifications for some steps:

1. Use the current changed strategy DID results to determine which post was the least effective over the scenario as described in Section 2.3.1.
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. Else 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 the results are less than the original base case model.

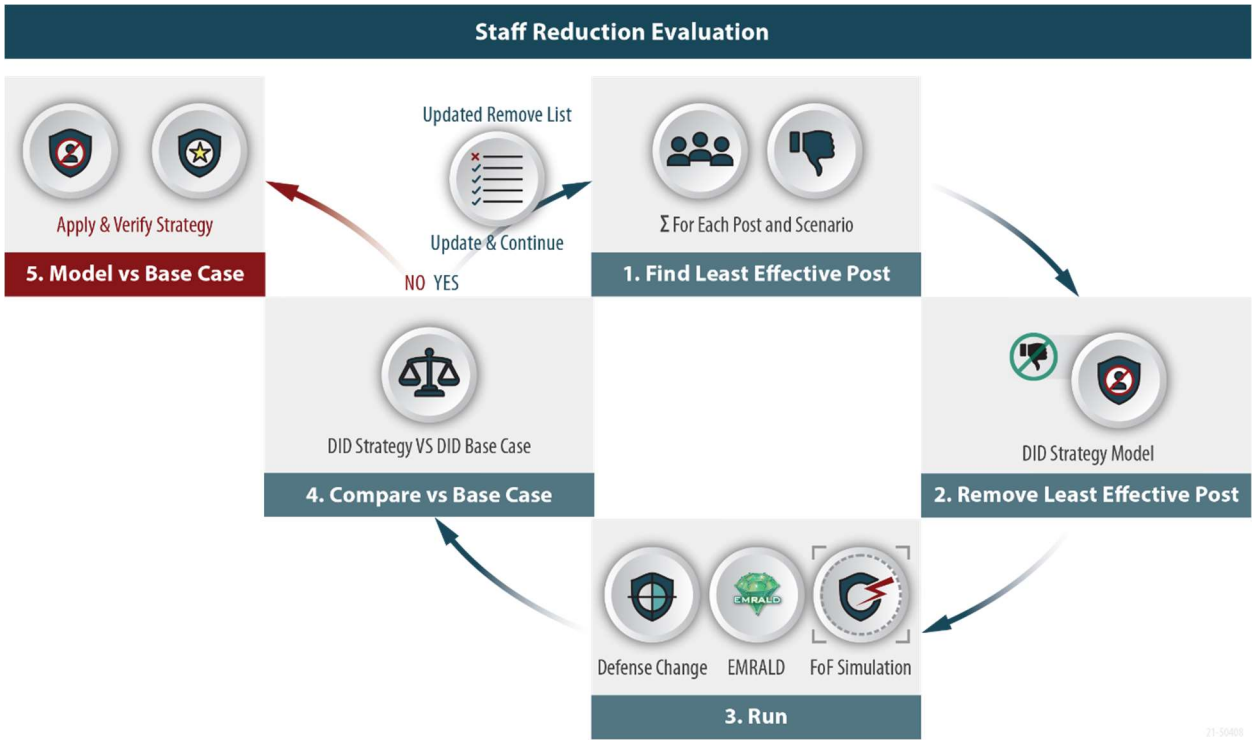


Figure 3. Process to evaluate staff reduction for a strategy change.

Once the process has stopped and validated, the posts in the "remove list" contain 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.

2.3.1 Evaluating Least Effective Post

Determining the "least effective" post is a manual process using the data provided to make performance-based choices; using a subject-matter expert could greatly enhance this process. When first entering the staff reduction loop, the model from the "Potential Strategy Evaluation" results in Section 2.2 are used, and for each successive evaluation, the current results from Step 3 (with posts removed) are used. The primary data for evaluating the "least effective" is the number of adversaries eliminated, but other criteria can also be added, as deemed useful by expert judgement. Other criteria could include noneffective engagement events, delay times, or detection/assessment capabilities. The evaluation is done through a simple scoring process normalized across each position across each scenario. The example below demonstrates the number of adversaries eliminated as the judging criteria, and the score for each post would be the number of adversaries eliminated divided by number of scenarios considered, in this case, four. The score for each post and each scenario is added to the probability and importance chart to help visualize the most contributing factors as shown in Table 4. While the scoring is useful in guiding the choice, a manual process informed by PPS experts would allow for identification of factors that may not be captured by modeling results.

Table 4. Combining post statistical data with scenario probabilities and importance.

Scenario	Adversary Success Prob.	Importance Measure	P1	P2	P3	P4
A	0.497	45.81%	0.75	0.25	0	0
B	0.29	26.73%	1	0	0	0
C	0.11	10.14%	0.5	0.25	0.25	0
D	0.188	17.33%	0.25	0.75	0	0
	MCUB	**Sum**				
	0.741909292	1.0000				

To pick the least effective post, consider the following:

1. Any posts that have no contribution to the scenario (as shown for P4 in yellow in Table 4 above).
2. Low overall contributors (such as P3).
3. Do not remove any posts that have a dominate contribution to any scenario (such as P1 and P2 above highlighted in green). If multiple guards have similar results, one or more could possibly be removed with the analysis results showing the effects of the removal.

2.3.2 Running the Modified Strategy Model

The post determined as the least effective is removed from the new strategy DID model scenarios or the previous run. Each successive run will eliminate one more responder and the results are used for evaluation. It is not necessary to perform the same number of runs for each scenario. The number of simulations to run should be determined by a convergence process. Simulations for a specific scenario can be run in batches. After each batch is ran, the change in MCUB is saved; if the rate of convergence meets the desired level (the change in MCUB flattens out), then enough simulations have been performed. After doing this for the "Potential Strategy Evaluation" of the DID model, the same number of runs for each scenario can be performed for each iteration of the post reduction. By running enough scenarios fora given convergence rate, an uncertainty value can be calculated. It may be necessary to adjust the responsibility of other posts to cover a critical aspect of the removed post.

2.3.3 Compare with DID Base Case

When comparing with the DID base case, if the following conditions are met, then the post's removal is not allowed, as follows:

A. If the potential strategy MCUB is worse than the DID base model.

B. If the probability of the most significant scenario of the potential strategy is higher than the most significant scenario probability of the DID base model. In this case, removing a different post may allow for continued reduction.

Comparing the potential strategy model against the DID model scenarios allows for a more detailed analysis of the results. Posts that may not see action in the base case cover sets are exercised and then produce data that can be used for to inform the potential change in the protective strategy.

2.3.4 Apply and Verify

Once all the excess posts are removed, a final analysis is performed. This analysis is done by removing the posts determined through the looping process from the initial potential strategy model without the DID modifications and running the model. This is then compared to the base case model. If the MCUB is less than the base case and no scenario probability is higher than the highest in the base case, then the PPS can be determined to be as effective as before the proposed change.

3. FOF-FLEX INTEGRATION

NRC regulations require "high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety" [4]. As such, the PPS of NPPs is required to protect against the act of radiological sabotage. As a licensing and inspection tool, NPPs are required to evaluate target sets. A target set is the minimum combination of equipment or operator actions (i.e., target set elements) that, if all are prevented from performing their intended safety function or prevented from being accomplished, would likely result in significant CD (e.g., non-incipient, non-localized fuel, which are melting and/or core destruction) or a loss of spent fuel pool coolant inventory and exposure of spent fuel, barring extraordinary actions by plant operations. The protection measures are considered as ineffective when a target set is sabotaged. This approach provides a clear and simplified acceptance criterion to the PPS design objective. However, it is understood that such a criterion contains a conservative assumption, which undermines the fact that there is a period of time from the moment a target set is damaged to the time when the plant undergoes a catastrophic failure and results in CD and possible offsite release.

The aforementioned time-margin can be utilized to perform mitigation actions in order to prevent CD. This section describes how FLEX mitigation strategies [10] can be leveraged for this purpose. These strategies rely on the use of FLEX portable equipment to provide backup power and/or heat removal from the reactor. It is well known that the preparation and operation of these portable equipment are done manually and, therefore, its timing of execution may vary significantly for different plants and scenarios [6]. In order to capture these timeline variations and assess the feasibility of these FLEX strategies, a dynamic framework of FOF and FLEX modeling approach is pursued.

Figure 4 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. This data is 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 pre-staged. Dynamic uncertainties of the FLEX preparation, as modeled in EMRALD, creates 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 this 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. Lastly, 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.

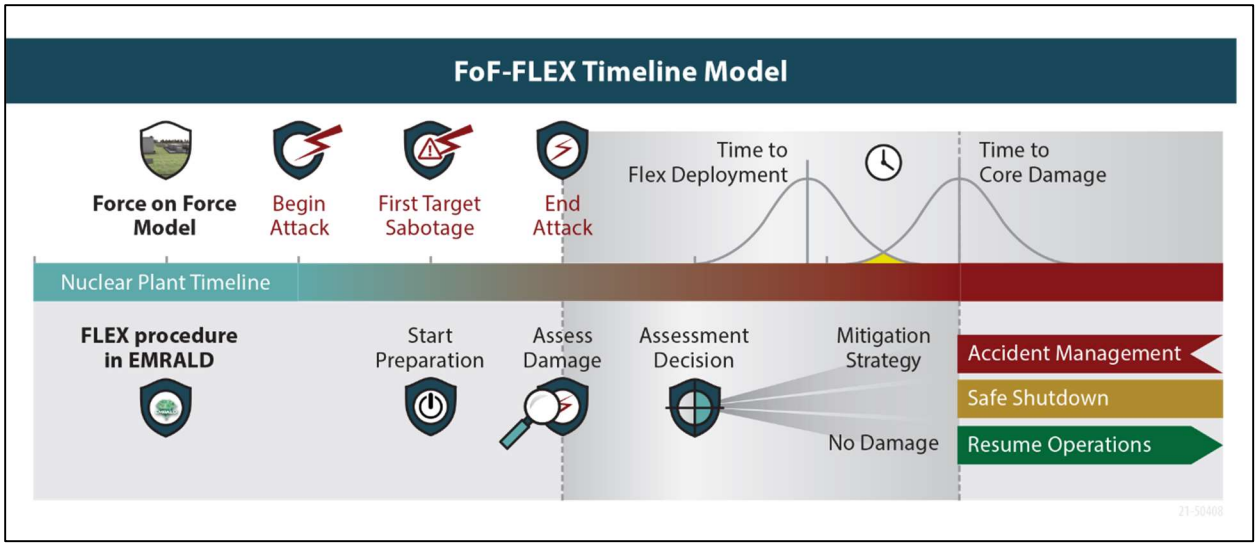


Figure 4. FOF-FLEX integration framework.

3.1 Case Study

3.1.1 Scenario Description

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) plant was developed in this case study. This case study does not use any plant proprietary data or information. 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 Figure 5, which is adopted from a station blackout (SBO) event tree for a PWR plant [9].

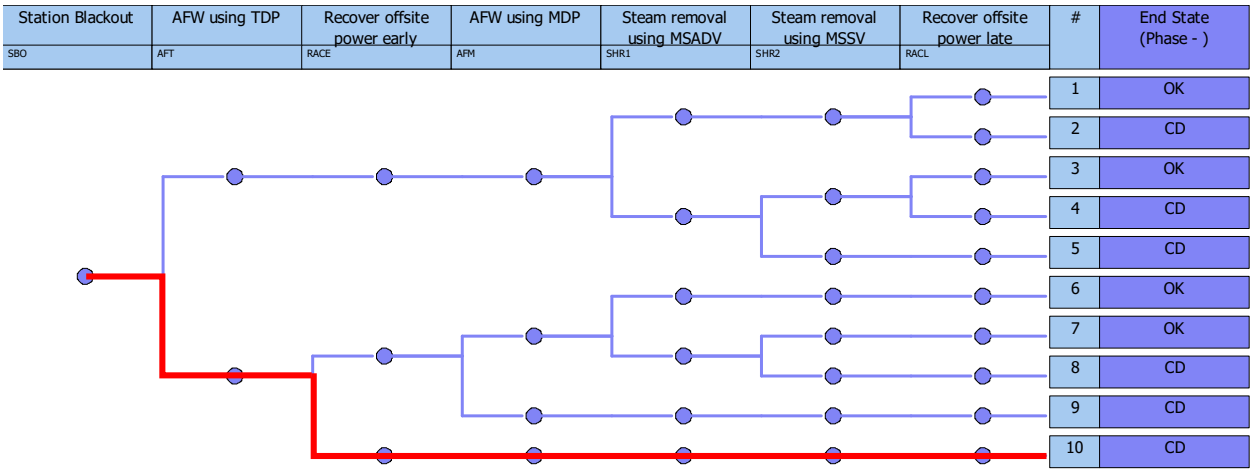


Figure 5. Sabotage scenario to inflict CD.

Target locations and the attack pathways to inflict the aforementioned CD progression are shown in Figure 6. An adversary sets explosives at an unmonitored grid tower outside of the nuclear plant complex to cause a loss-of-offsite-power (LOOP) event. Meanwhile, a group of armed adversaries enters the complex to sabotage the emergency diesel generators (EDGs) to cause an SBO event and damage the turbine driven pumps (TDPs) to disable the plant's passive heat removal capability. Adversaries then

proceed to sabotage the FLEX diesel generators (DG) and FLEX pumps to disable the plant's mitigation strategy completely. The plant has its physical protection program in place, consisting of the intrusion detection system (IDS), delay barriers, and both the stationary and mobile response force. These protection elements are not shown in Figure 6 to provide a visual clarity on the attack path and target locations. The PRA models show if all of these targets are sabotaged, the nuclear plant will experience the CD state within an hour [9].

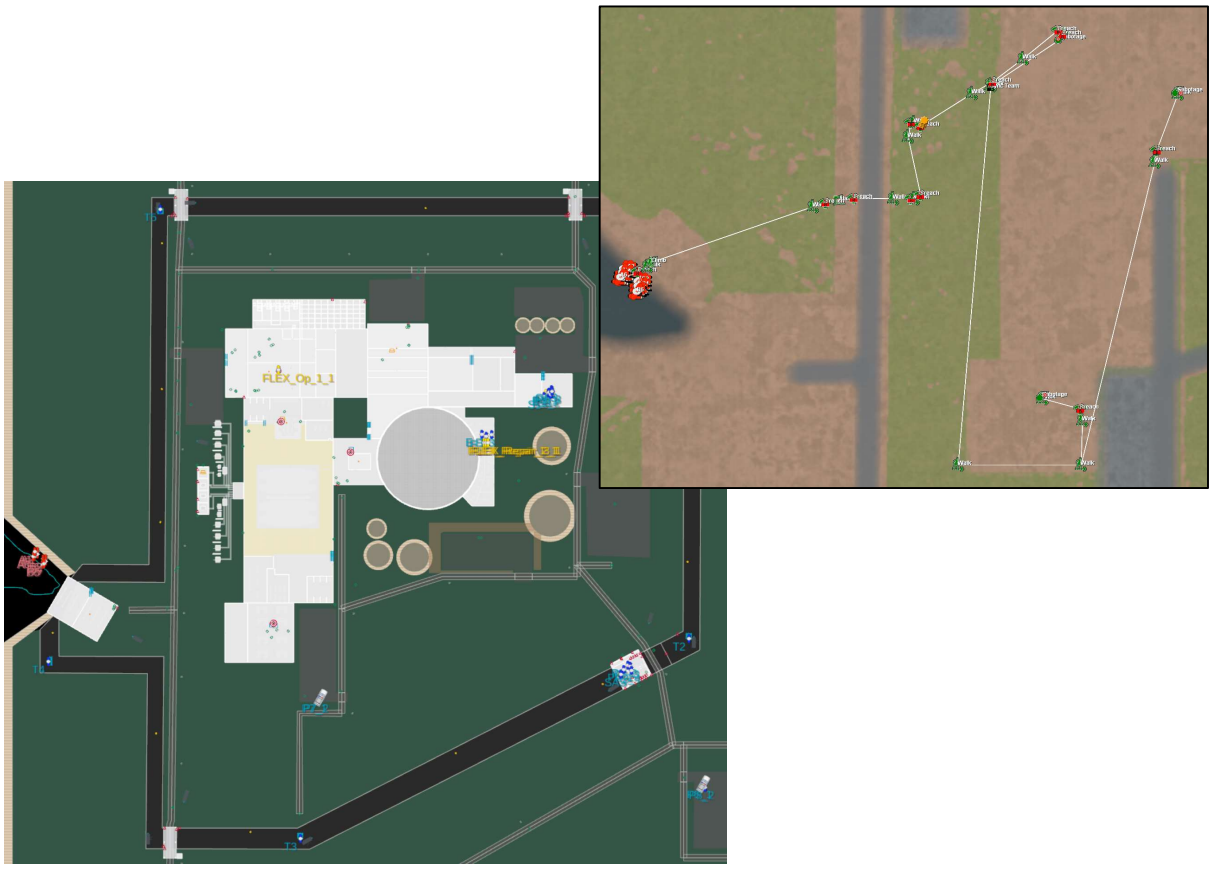


Figure 6. Facility layout and the attack plan in the FOF model.

Multiple attack scenarios are investigated to analyze the overall plant physical security posture as explained in Section 2.1. For the purpose of illustration, a total of four attack scenarios are included in this study. Two attack scenarios with the same set of sabotage targets as shown in Figure 6 and varying attack paths are developed. An additional attack scenario is created in which the adversaries split into two teams attacking from two separate directions simultaneously. The target set in this scenario is different from the one in Figure 6. Detailed descriptions of these attack scenarios are given in the Appendix A. For this demonstration, it is assumed these few scenarios are a complete cover set as described in Section 2.1.1; although, for an actual implementation, it is likely many more scenarios would be included.

A list of all possible outcomes from the attack scenario is shown in Table 5. 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 are sabotaged, the reactor core is assumed to be damaged. Similarly, if all design basis safety systems are sabotaged, the FLEX extended loss-of-ac-power (ELAP) strategy is assumed successful if all the necessary backup equipment are intact. The timeframe for performing these FLEX strategies is taken from a reference study [9].

Table 5. Possible attack outcomes.

No	System Availability				Mitigation Strategy
	EDG	TDP	FLEX DG	FLEX Pump	
1	✓	✓	✓	✓	Safe shutdown
2	✓	✓	✓	X	Non-transient shutdown
3	✓	✓	X	✓	Non-transient shutdown
4	✓	✓	X	X	Non-transient shutdown
5	✓	X	✓	✓	FLEX pump strategy
6	✓	X	✓	X	N/A (CD)
7	✓	X	X	✓	FLEX pump strategy
8	✓	X	X	X	N/A (CD)
9	X	✓	✓	✓	FLEX generator strategy within 11 hours
10	X	✓	✓	X	FLEX generator strategy within 11 hours
11	X	✓	X	✓	N/A (CD)
12	X	✓	X	X	N/A (CD)
13	X	X	✓	✓	FLEX ELAP strategy within 1 hour
14	X	X	✓	X	N/A (CD)
15	X	X	X	✓	N/A (CD)
16	X	X	X	X	N/A (CD)

3.1.2 FLEX Implementation in EMRALD

Figure 7 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 simulation such as the weapons' probability of kill (PK), 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 Simajin 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 *Asses_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 sub diagram. The *Check_FLEX_EDG* event is initiated if the *FLEX_DG* sub diagram returns a value which indicates the success of 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 one hour. This state leads to the decision of whether 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.

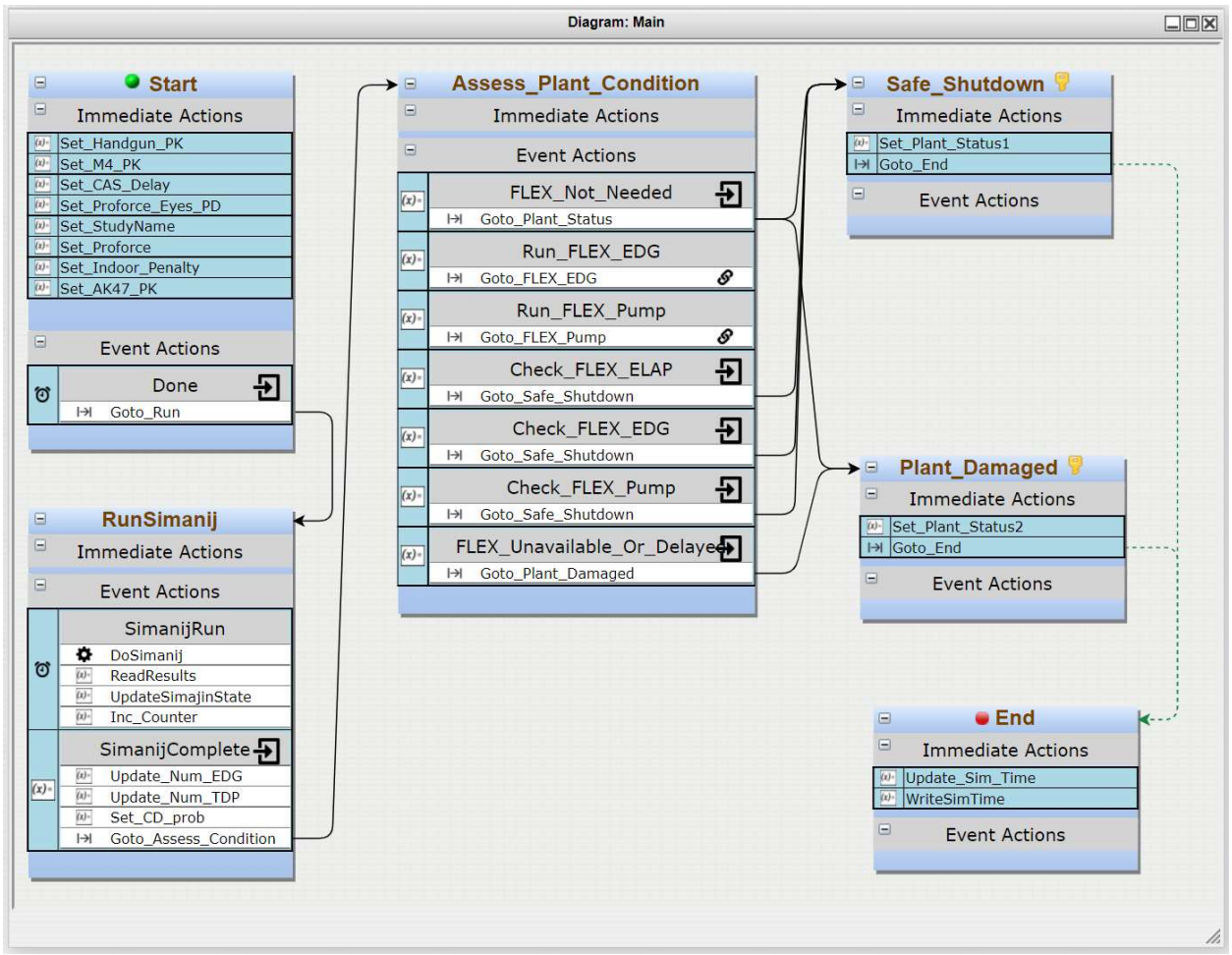


Figure 7. Main EMRALD diagram.

Table 6 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 are done prior to executing the FLEX mitigation strategy, as illustrated in the “Start Preparation” step in Figure 4. 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 6.

Table 6. FLEX procedure.

Number	Steps	Notes
1	Get keys and open doors	Preparation
2	Assess condition of plant system & equipment	Execution
3	Contact Strategic Alliance for FLEX Emergency Response (SAFER) control center to inform the extended-loss-of-ac-power event	Execution
4	Connect FLEX steam generator (SG) makeup pumps' hose	Preparation
5	Establish configuration to support FLEX 480V ac installation	Execution
6	Connect FLEX cables to 480V Motor Control Centers (MCCs)	Preparation
7	Open ALL breakers on MCCs	Execution
8	Connect FLEX RCS 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 RRC	Execution
14	Ensure support equipment are staged	Preparation
15	Establish communication	Execution

Some of the actions listed in Table 6 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 to 3 and the delay in preparing the equipment, which includes Steps 5, 9, 11 and 15, are included in the FOF simulation. The remainder of the FLEX mitigation actions are modeled in EMRALD as shown in Figure 8 and Figure 9 for FLEX generators and FLEX pumps, respectively.

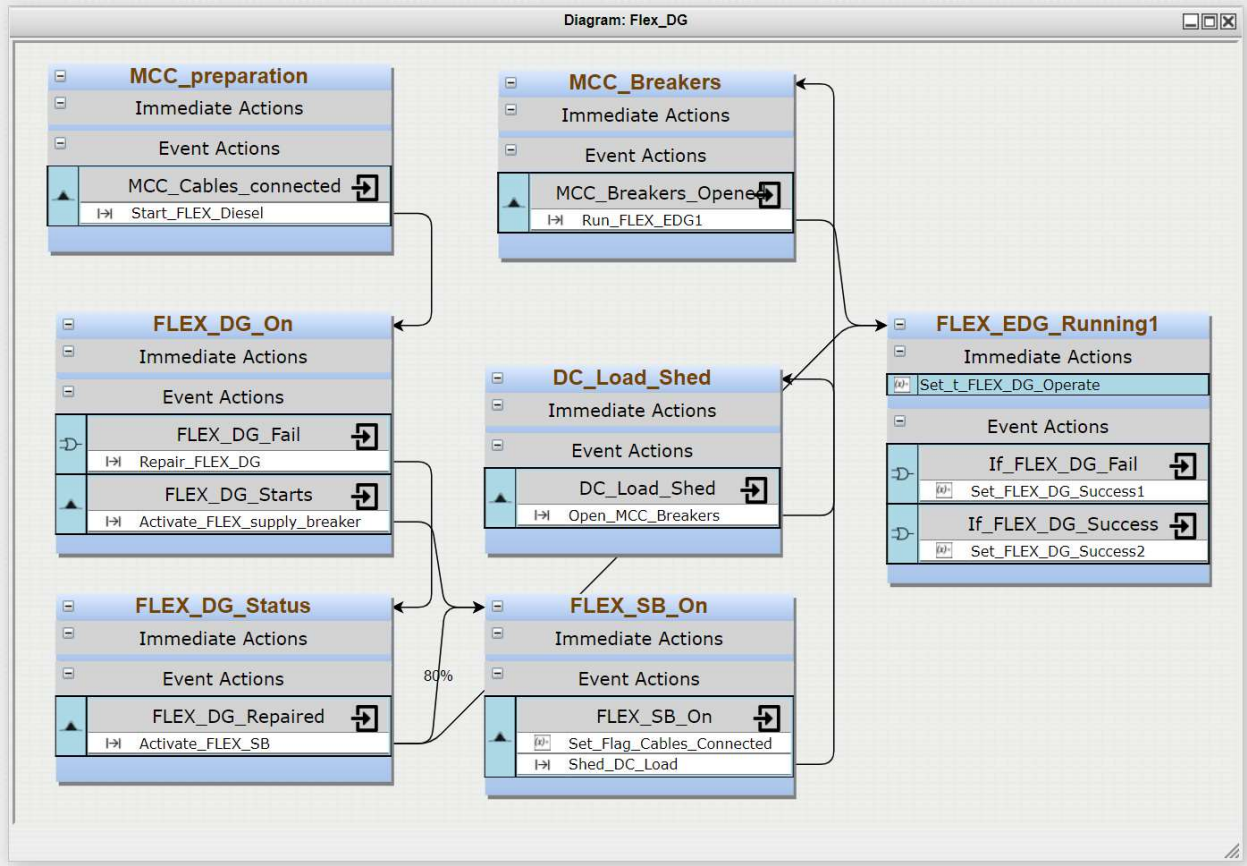


Figure 8. EMRALD diagram for FLEX generators.

In the FLEX generator strategy, the *MCC_preparation* stage samples the time required for a FLEX operator to connect the FLEX cables to 480V MCCs. After the cables are connected, the simulation continues to the *FLEX_DG_On* state. If the FLEX generators fail 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. After the generators run, the supply breaker is turned on, a direct current (DC) load shed is performed, and the MCC breakers are opened. The time required to perform all these actions is added with the mobilization time from the FOF simulation and recorded as *t_FLEX_DG_Operate* in the *FLEX_EDG_Running1* state.

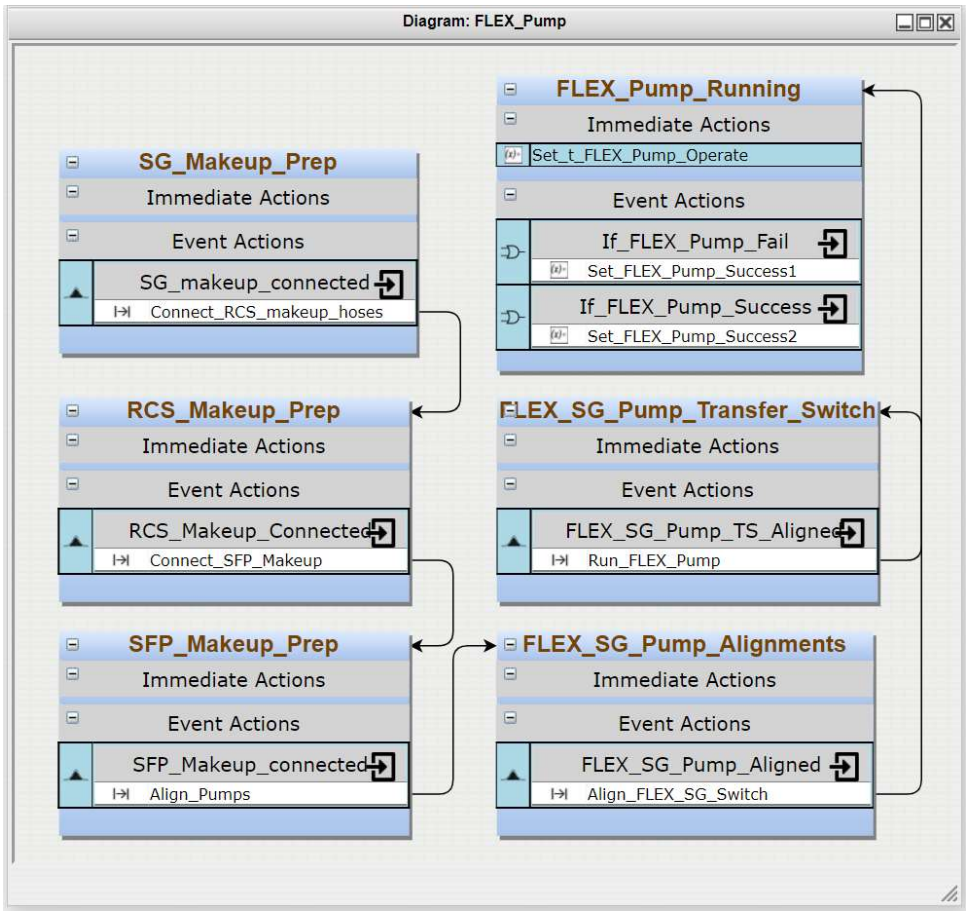


Figure 9. EMRALD diagram for FLEX pumps.

If the coolant circulation capability is lost, the FLEX pump strategy is initiated. As shown in Figure 9, this strategy begins with connecting hoses between the FLEX pumps and the coolant inlet ports. After the hoses are connected, the operator aligns the FLEX pumps and the transfer switch. The timing for each of these actions are 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.

It is assumed FLEX equipment are installed in pairs for redundancy. The operational states of both FLEX generators are modeled in EMRALD as shown in Figure *10*. The *FLEX_DG1_Standby* and *FLEX_DG2_Standby* states are run when the simulation starts. When a demand for FLEX generators comes (i.e., when the simulation enters *FLEX_DG_On* state in Figure 8), the *FLEX_DG1_Demand* and *FLEX_DG2_Demand* events initiate. It is assumed the generators have a 1E−2 probability of failing to start. If they start successfully, the *FLEX_DG1_Active* and *FLEX_DG2_Active* states are initiated for each of the generators respectively. The *FLEX_DG1_FR* and *FLEX_DG2_FR* are events based on the specified failure rate of the generators. In this case study, it is assumed the generators have a failure rate parameter lambda of 1E−4 with a mission time of 24 hours. When the generators fail—either fail to start or fail to run—for 24 hours, the *FLEX_DG1_Fail* and *FLEX_DG2_Fail* states are initiated for each generator. If the operator manages to repair it (i.e., when the simulation enters the *FLEX_SB_On* state in Figure 8), the *FLEX_DG1_Repaired* and *FLEX_DG2_Repaired* events are activated, and the generators return to their operational state.

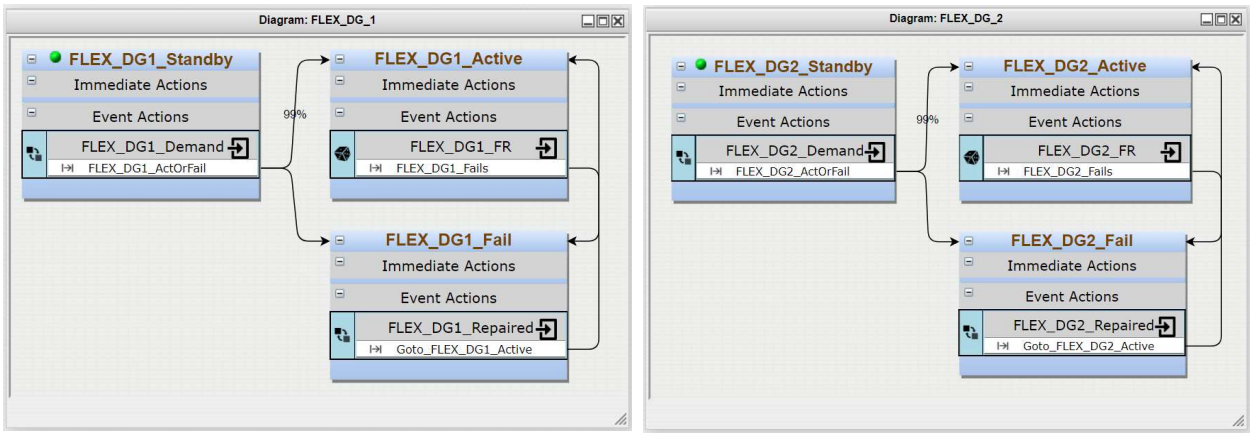


Figure 10. Diagrams of FLEX generator's operational states.

Figure 11 shows the diagrams for the FLEX pumps' states. When demand comes (i.e., when EMRALD enters the *FLEX_Pump_Running* state in Figure 9), the *FLEX_AFW_P1_Demand* and *FLEX_AFW_P2_Demand* events are activated. These events start the pumps with a 0.99 success probability. The FLEX pumps' failure rate is assumed the same with the FLEX generators' failure rate (i.e., a lambda of 1E−4 for a continuous operation time of 24 hours). If the pumps fail to start or fail to run, they remain in the failed state until the simulation ends.

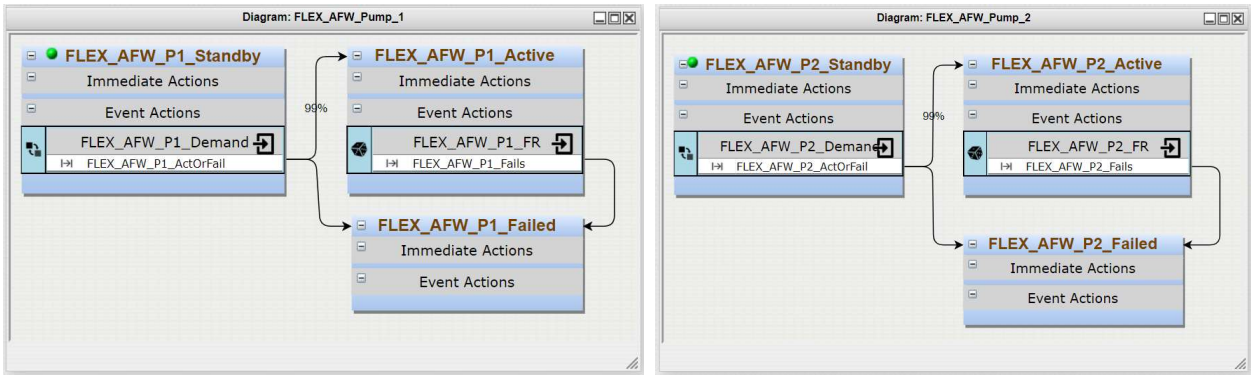


Figure 11. Diagrams of FLEX pump's operational states.

Following the generator and pump's availability as detailed in Figure 10 and Figure 11, simple fault trees of redundant FLEX generators and pumps are modeled in EMRALD as shown in Figure 12. The state of the top event in these fault trees determines the availability of backup power generation and backup cooling circulation capabilities.

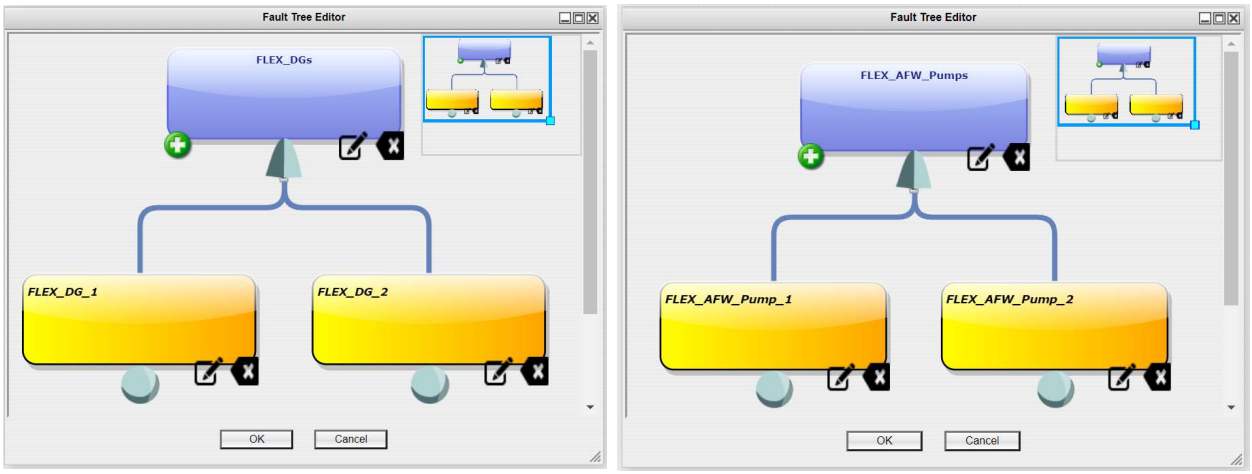


Figure 12. Fault tree diagrams of FLEX equipment.

3.2 Results and Discussion

3.2.1 Convergence Analysis

Multiple runs of simulations for each attack scenario are needed to obtain the probabilistic risk from that scenario. When obtaining probability values using simulations, it is important to ensure a sufficient number of simulations are performed that provide a reliable estimate of the probability value. Too few simulations might result in a probability value that might change significantly with additional simulations. Too many simulations are a waste of computational resources with no significant insights in probability results. A convergence analysis was conducted to determine the minimum number of runs needed for reliable conditional CD probability (CCDP) values. The results are shown in Figure 13–Figure 16 for the attack Scenarios A–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.

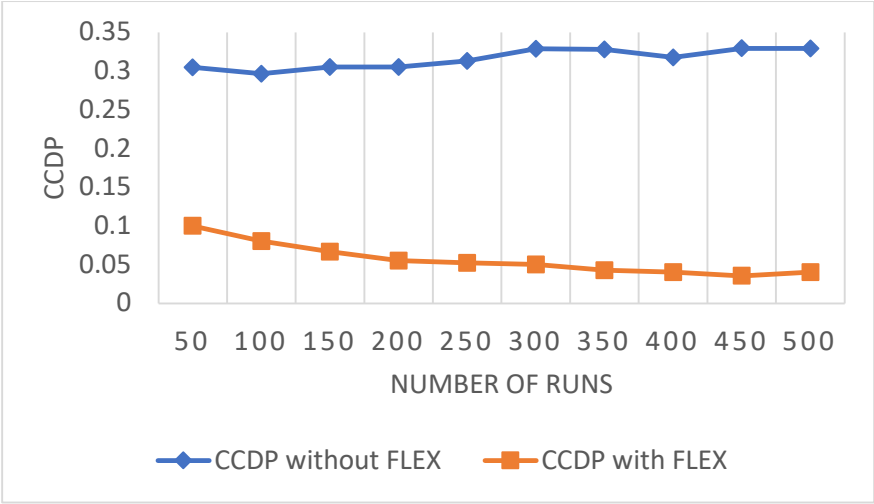


Figure 13. Convergence analysis for the attack Scenario A.

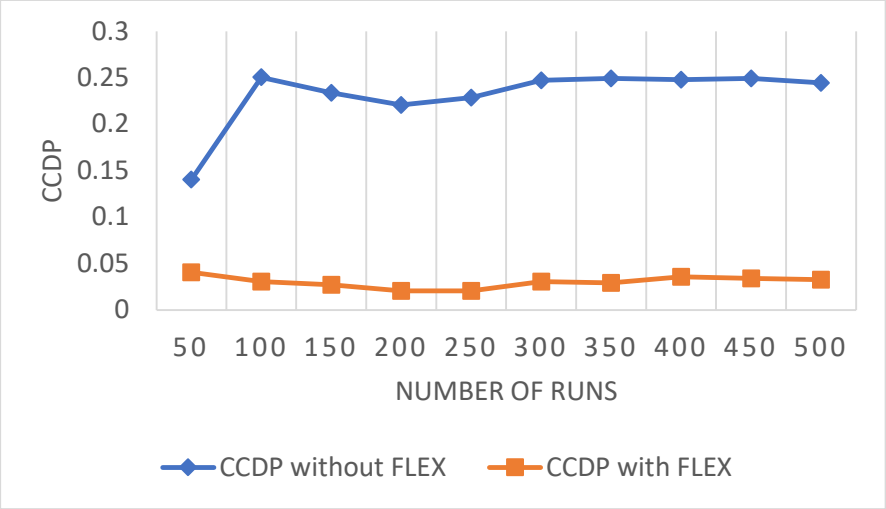


Figure 14. Convergence analysis for the attack Scenario B.

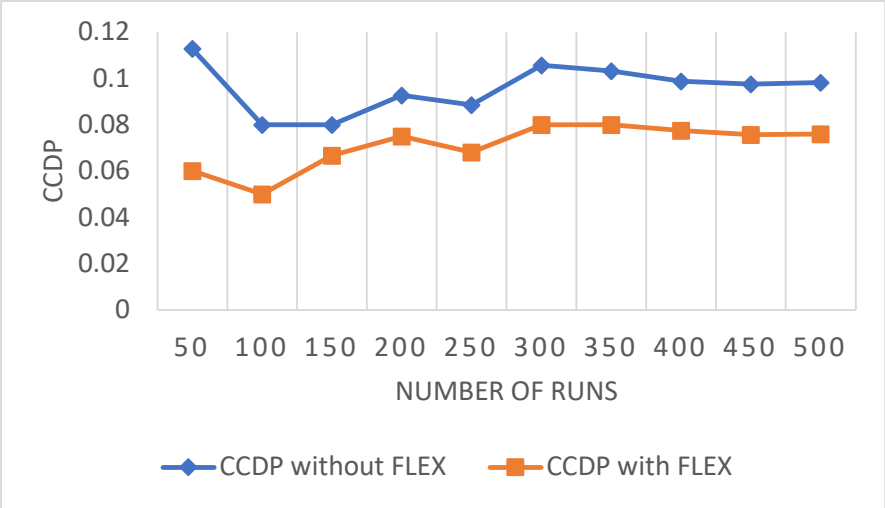


Figure 15. Convergence analysis for the attack Scenario C.

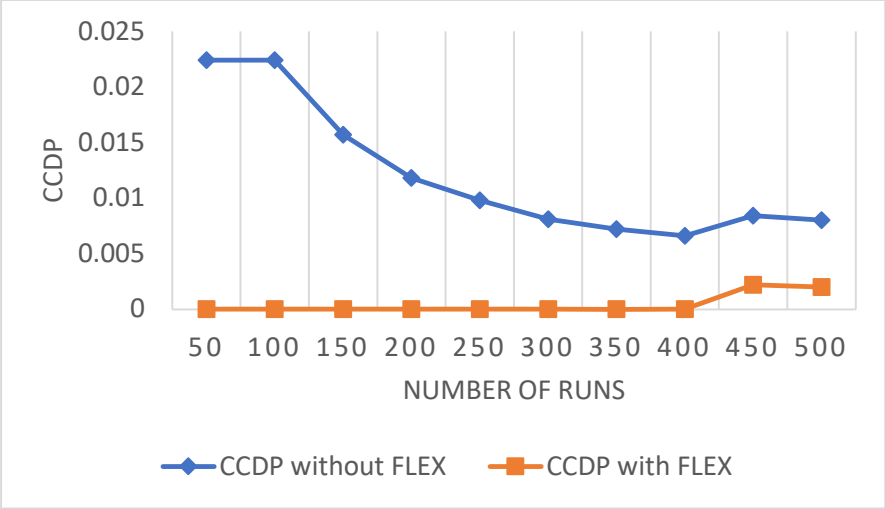


Figure 16. Convergence analysis for the attack Scenario D.

3.2.2 Probability Calculation

The integrated FOF-FLEX model was simulated for the initial attackers. A total of 500 simulations were run for each of the four attack scenarios. Results for the first attack scenario are summarized in Table 7. 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 FLEX strategy is not used may be taken from plant-specific probabilistic risk assessment (PRA) models. However, these values are reasonably assumed for the hypothetical plant used in this study. Meanwhile, the CD probabilities with FLEX strategy are computed from the EMRALD simulation when FLEX equipment fail to operate or is operated beyond the conservative time limit of 1 hour. Some of the attack outcomes in Table 7 did not occur because the adversaries are assumed to strike target components in successions. For example, if adversaries have not sabotaged the first component in their target list, they will not skip it to attack the second component.

Table 7. CCDP calculations for the first attack scenario with DBT adversaries.

Scenario Number	System Availability				Number of events	FOF 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 7 shows using FLEX mitigation strategy reduces the adversary success probability for this attack scenario. However, this result is for only one attack scenario. Results for other attack scenarios are tabulated in the Appendix A and are summarized in Table 8. This table shows using FLEX strategy reduces the overall adversary success probability from sabotage attacks by two orders of magnitude. It illustrates the probability margin obtained from utilizing backup equipment to mitigate the adverse effects of security incidents. This margin can be leveraged to optimize the physical protection system, particularly the number of armed responders, through the methodology as explained in Section 2.

Table 8. Overall failure probabilities of the DBT 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

As explained in Section 2, attack scenarios beyond the established DBT are investigated to analyze the physical security effectiveness beyond the outermost layer of protection, termed as DID. For this demonstration, the DID scenarios are simulated by increasing the number and attack capabilities of the adversary team. Details of DBT and beyond-DBT attacks for each scenario are given in the Appendix A. For a beyond-DBT attack, results for the first attack scenario are given in Table 9. The outcomes with zero probabilities are collapsed to highlight the more significant data. Comparing Table 7 and Table 9 demonstrates adversaries are more likely to penetrate through the PPS and damage the targets with a beyond-DBT 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.

Table 9. CCDP calculations for the first attack scenario with beyond-DBT adversaries.

No	System Availability				Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
	EDG	TDP	FLEX DG	FLEX Pump				
1	Y	Y	Y	Y	276	0.552	0.552 x 1E−6	0.552 x 1E−6
2–8	Y	*	*	*	0	0	0	0
9	N	Y	Y	Y	62	0.124	0.124 x 4E−2	0.124 x 1.54E−4
10–12	N	Y	*	*	0	0	0	0
13	N	N	Y	Y	142	0.284	0.284 x 1	0.284 x 1.83E−4
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	0.329	4E−2

Figure 17 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 FLEX operation has two distinct peaks corresponding to the timing when safety functions of DGs and TDP pumps are lost.

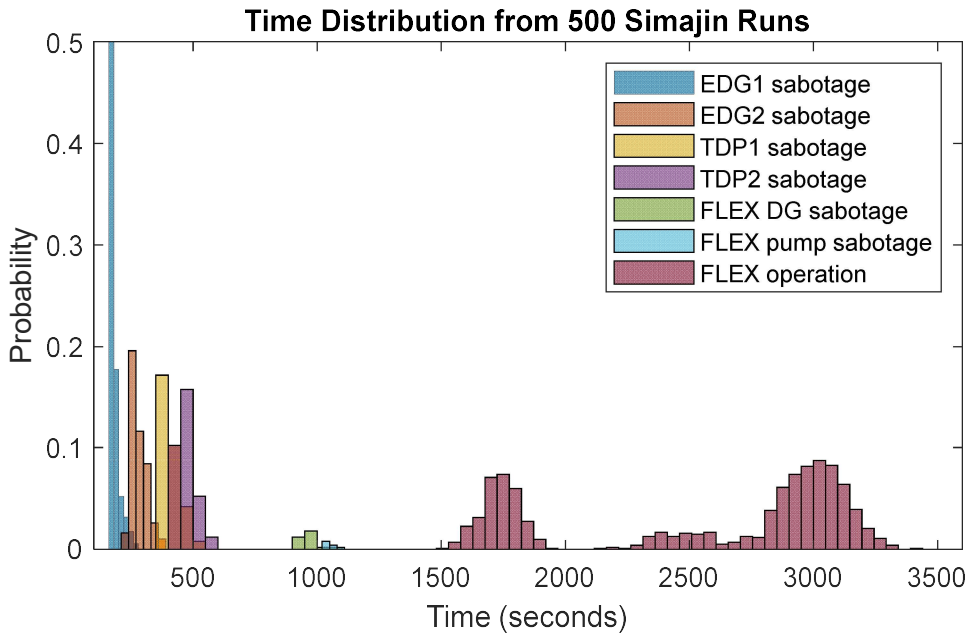


Figure 17. Time distribution of events in Scenario A.

The methodology shown in Table 9 is repeated for other attack scenarios. Detailed results are given in the Appendix and are summarized in Table 10. As expected, the beyond-DBT attacks increased the CCDP for each attack scenario.

Table 10. Overall adversary success probability of beyond-DBT attack scenarios.

Scenarios	**Importance Measure**		**CCDP**	
	Without FLEX Strategy	**With FLEX Strategy**	**Without FLEX Strategy**	**With FLEX Strategy**
Scenario A	38.48%	14.25%	3.29E−01	4.00E−02
Scenario B	28.60%	11.61%	2.45E−01	3.26E−02
Scenario C	11.46%	27.08%	9.80E−02	7.60E−02
Scenario D	21.46%	47.06%	1.84E−01	1.32E−01
Total	100.00%	100.00%	6.27E−01	2.55E−01

3.2.3 Evaluating Least Effective Post

The likelihood of a responder to neutralize adversaries in an attack scenario is obtained by dividing the number of neutralization to the total number of neutralization done by the protective force. This value is calculated for each post. Posts are then ranked based on their neutralization probability in an ascending manner. In this sense, posts having high ranks are deemed crucial to protect the target set for that attack scenario. Figure 18 visualizes the ranks for the initial protective force on all attack scenarios where the x-axis denotes the ID of the post in the FOF model, and the y-axis is the rank of neutralization effectiveness. This result is used to determine the least effective post as described in Section 2.3.1. The least effective post in this initial run is determined as T2 because it is not significant in Scenarios A and B and is relatively less important than other posts in Scenarios C and D.

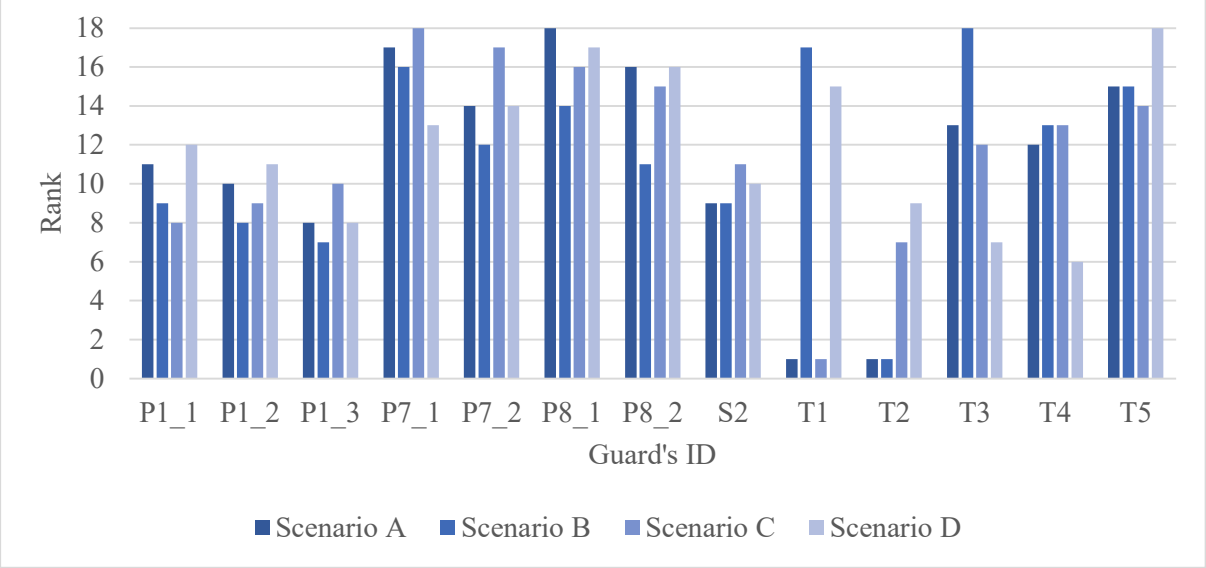


Figure 18. Ranks of adversary neutralization across attack scenarios.

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 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 as described in Section 2.3. The iterative process of determining the least effective post is detailed in the Appendix C. Through this iterative process, it is found 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 Figure 19. It shows the adversary success probability when five posts are removed exceeds the initial adversary success probability, therefore that configuration is not selected.

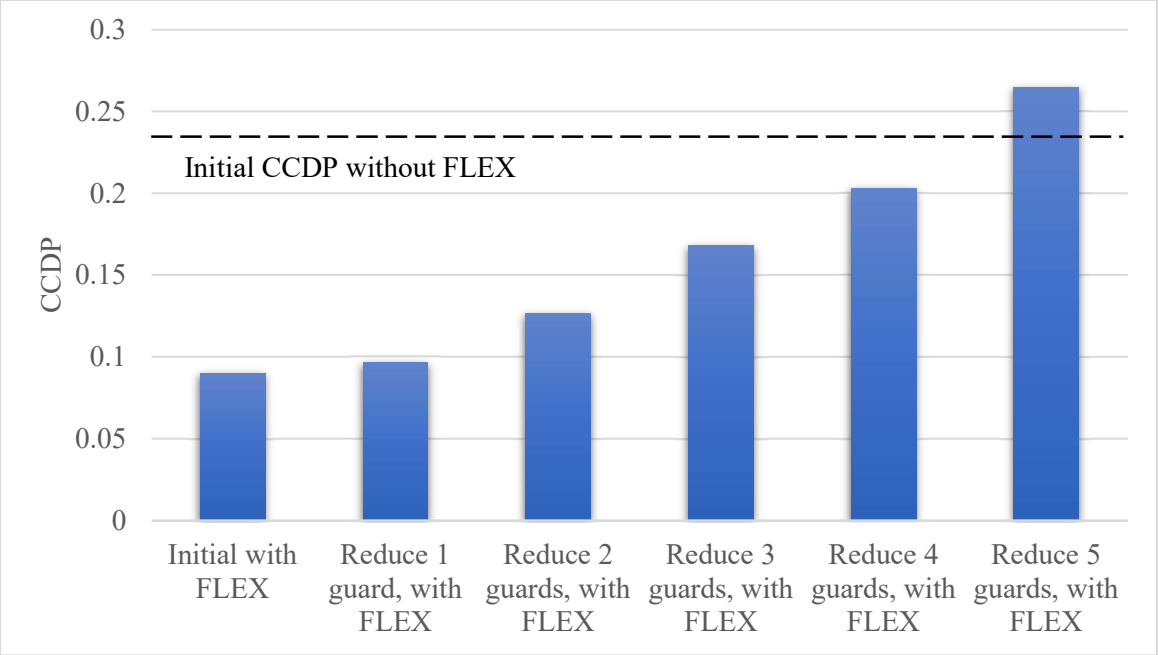


Figure 19. Adversary success probability and margin.

The methodology of security optimization in this study is deemed conservative because it elevates the adversary's capabilities beyond the DBT. This approach is selected to evaluate the PPS DID elements, without running many computationally expensive FOF simulations. The optimized PPS is then validated using DBT attacks to verify it does not increase the adversary success probability relative to the initial PPS configuration. The result of this verification is shown in Figure 20. The metric used in the figure is the total CCDP from all attack scenarios. When FLEX strategy is incorporated to mitigate the adverse outcomes of DBT attacks, the total adversary success probability scales down by an order of magnitude.

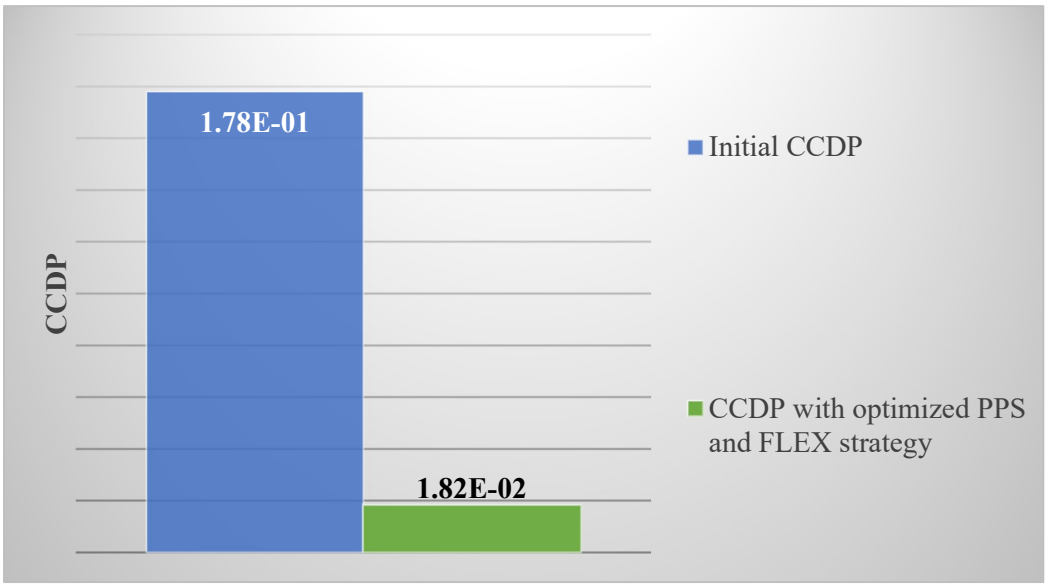


Figure 20. Adversary success probability comparison for DBT attacks.

4. CONCLUSION AND FUTURE WORK

This report describes the research and development being performed at INL towards a dynamic modeling and simulation framework to enable physical security optimization at commercial NPPs. The framework is based on EMRALD, the dynamic modeling tool, and is demonstrated for applications that can result in physical security optimization. Two main applications are presented: (1) physical security optimization by staff reduction analysis and (2) extension of the existing FOF-FLEX integration framework across (a) another commercially available FOF tool and (b) a comprehensive set of attack scenarios.

The presented analysis is focused on optimizing physical security posture at NPPs by performing reduction in number of armed guards. The optimization framework starts with evaluating the effectiveness of the current physical security posture, followed by a DID analysis and staff reduction evaluation. The staff reduction evaluation analysis entails an iterative framework that identifies the least effective post in the plant physical security posture across an extensive set of potential attack scenarios. The framework then recommends removal of the least effective post but only if the removal has minimal impact on the performance effectiveness of the overall security posture.

INL's existing framework for modeling FLEX portable equipment is extended to integrate with FOF modeling in another popular commercial tool, Simajin. This report presents several case studies of modeling adversarial attacks aimed at causing a radiological release by sabotaging the plant's critical assets at a hypothetical PWR. The results demonstrate that even in the extreme case of a successful adversarial attack, deploying FLEX equipment can result in a significantly high likelihood of preventing radiological release. The modeling and simulation framework of integrating FLEX equipment with FOF models enables the NPPs to credit FLEX portable equipment in the plant security posture, resulting in an efficient and optimized physical security. The presented work has resulted in now integrating INL's dynamic simulation tool, EMRALD, with three FOF simulation tools SCRIBE3D, AVERT, and Simajin, of which the latter two are currently being used by a majority of commercial NPPs across the nation for their FOF modeling. Integrating EMRALD with these tools paves way for the wide implementation of INL's physical security optimization framework at commercial NPPs.

Ongoing and future efforts in this area include: (1) implement the framework on a plant's specific physical security posture and FLEX equipment; (2) model the FLEX equipment and enclosure as a target set in the physical security posture, and (3) integrate human reliability analysis in the dynamic model.

5. REFERENCES

1. Pacific Gas and Electric Company. 2018. “PG&E Company 2018 Nuclear Decommissioning Costs Triennial Proceeding Prepared Testimony – Volume 1.” 18-12 (U 39 E), PG&E Company. https://analysis.nuclearenergyinsider.com/pge-seeks-decommissioning-head-start-cost-estimates-rise.
2. U.S. Nuclear Regulatory Commission. 2020. “Emergency Preparedness in Response to Terrorism.” About Emergency Preparedness. Last modified November 13, 2020. https://www.nrc.gov/about-nrc/emerg-preparedness/about-emerg-preparedness/response-terrorism.html#one.
3. U.S. Nuclear Regulatory Commission. 2021. “PART 73—Physical Protection of Plants and Materials.” Regulations (NRC, 10 CFR). Last modified March 24, 2021. https://www.nrc.gov/reading-rm/doc-collections/cfr/part073.
4. U.S. Nuclear Regulatory Commission. n.d. “Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage.” Regulations (NRC, 10 CFR), Part Index. Last modified March 24, 2021. https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0055.html.
5. Garcia, M. L. 2005. *Vulnerability Assessment of Physical Protection Systems*. Oxford: Butterworth-Heinemann.
6. Nuclear Energy Institute. 2017. “Guidance for Optimizing the Use of Portable Equipment.” NEI 16-08, Nuclear Energy Institute.
7. Idaho National Laboratory. n.d. “EMRALD.” Accessed July 28, 2021. https://emrald.inl.gov/SitePages/Overview.aspx.
8. RhinoCorps Ltd. Co. 2021. “Rhino Corps Homepage.” Accessed July 28, 2021. https:// https://www.rhinocorps.com.
9. Kang, D., and S. Chang. 2014. “The safety assessment of OPR-1000 nuclear power plant for station blackout accident applying the combined deterministic and probabilistic procedure.” Nuclear Engineering and Design 275 (August): 142–153.
10. Nuclear Energy Institute. 2016. “Diverse and Flexible Coping Strategies (FLEX) Implementation Guide.” NEI 12-06, Rev. 4, Nuclear Energy Institute.Smith, C.L. et al. 2008. "Systems Analysis Programs for Hands-On Integrated Reliability Evaluations (SAPHIRE) Technical Reference." INL/EXT-05-00327, Rev. 1, Idaho National Laboratory.
11. Smith, C.L. et al. 2008. "Systems Analysis Programs for Hands-On Integrated Reliability Evaluations (SAPHIRE) Technical Reference." INL/EXT-05-00327, Rev. 1, Idaho National Laboratory. https://inldigitallibrary.inl.gov/sites/sti/sti/4096539.pdf.

Page intentionally left blank

Appendix A
Description of Attack Scenarios

Page intentionally left blank

Appendix A
Description of Attack Scenarios

1. Scenario A (Disrupt Power)

This attack scenario is pictured in Figure A-1. The adversaries are comprised of two elements: Alpha, a six-man team, and Bravo, a six-man team. Alpha and Bravo elements all gain access via insertion between Sector 8 and 9, just north of the inlet building. Alpha and Bravo elements continue path to breach protected area (PA) fence in Sector 9.

The Alpha and Bravo elements continue to the diesel generator building where they explosively breach into that building and sabotage the most southern and then most northern generators. Then Alpha and Bravo elements make their way to the western power plant door and explosively breach. Both elements then make their way to sabotage TDPs 1 and 2.

At this point, both elements go back out to the previously breached power plant door and head south around the turbine building to gain access to the boiler room door. This is where Alpha and Bravo elements split. Alpha team explosively breaches the boiler room door and makes their way to the prepositioned FLEX equipment within the boiler room to destroy that equipment. The Bravo element makes their way north to the steam room door where they will explosively breach and enter the steam room to destroy the prepositioned FLEX equipment in this room.

Scenario A DBT is the same as above except Alpha and Bravo teams are each three-man teams.

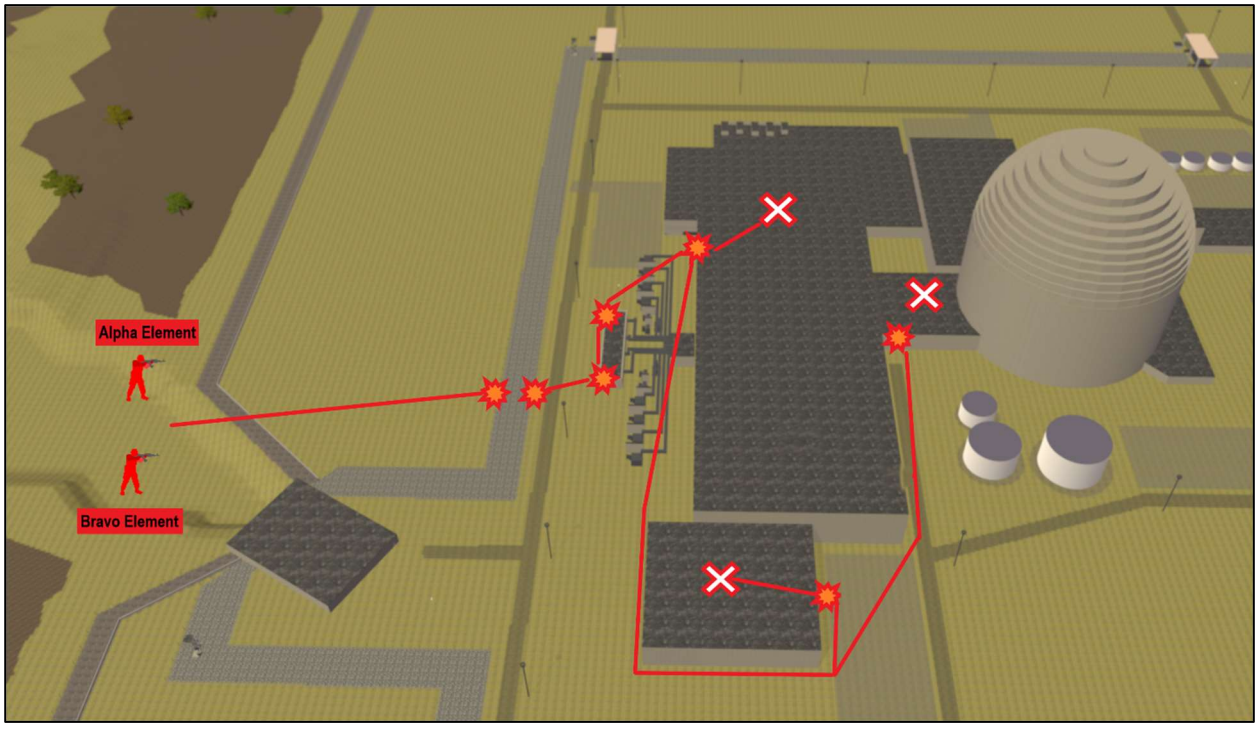


Figure A-1. Attack Scenario A.

2. Scenario B (Foot Aux and Intake)

This attack scenario is pictured in Figure A-2. The adversaries are comprised of two elements: Alpha, a six-man team, and Bravo, a six-man team.

Alpha team mechanically breaches the northern fence in Sector 12. They continue south to explosively breach the PA and the PA inner fence in Sector 12. Alpha proceeds south to Door18 where the explosively breach and gain access to the aux building cooling system control and the target set in the aux building. Alpha will then proceed back out of the aux building and go west around the turbine building going for the boiler room door. They will either explosively breach this or if Bravo team has already beached this, Alpha will enter and either sabotage the prepositioned FLEX equipment in this area or provide cover for Bravo team if they have arrived already.

Bravo waits for Alpha team to activate an alarm then gains access via insertion with mechanical breaches to the LAA and PA outer fences in Sector 9 just north of the intake building. Bravo then explosively breaches the PA inner fence and proceeds to door D-30-001, where they explosively breach and gain access to the intake manifolds. Bravo will then exit the intake building and head for the southeast boiler room door. They will either explosively breach this door or if Alpha team has already breached this door, Bravo will enter and assist in the sabotage of the prepositioned FLEX equipment inside.

Scenario B DBT is the same as above except Alpha and Bravo teams are each three-man teams.

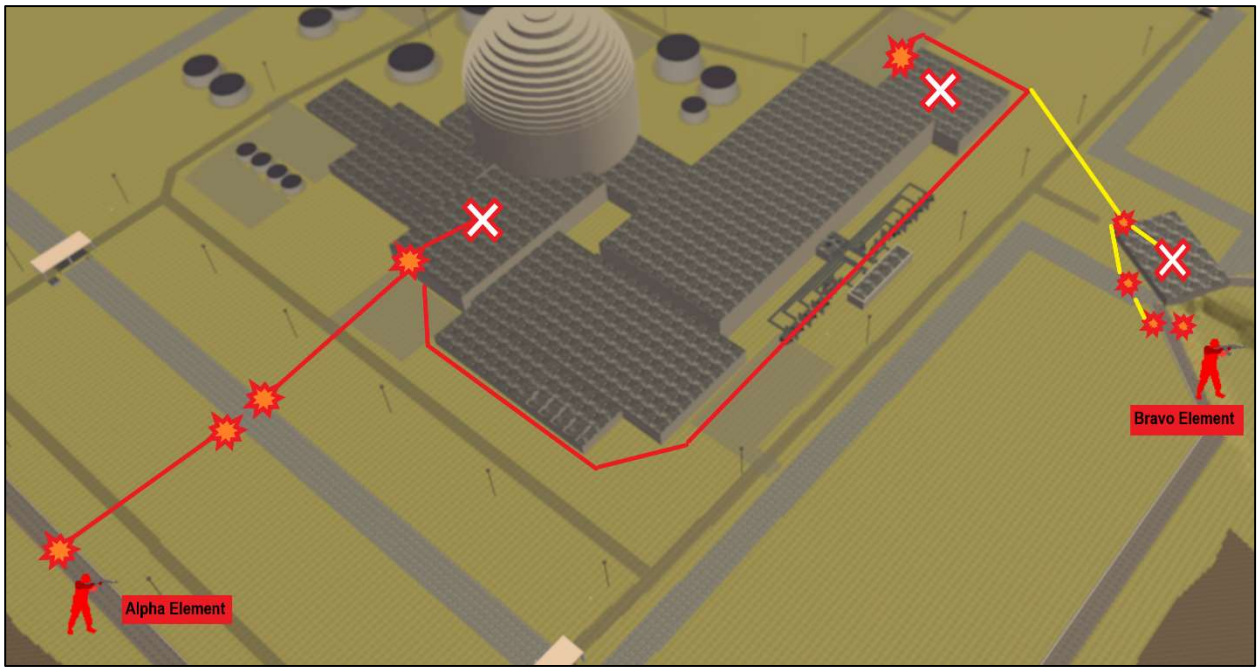


Figure A-2. Attack Scenario B.

3. Scenario C (Foot Steam Valve)

This attack scenario is pictured in Figure A-3. The adversaries are comprised of three elements: Alpha, a six-man team; Bravo, a six-man team; and Charlie, a one-man team giving overwatch support.

Alpha team explosively breaches the PA fences between Sectors 5 and 6. The team then makes their way north to the steam room door and explosively breaches gaining access to the door between the turbine building and the steam room building. This door is also explosively breached giving access to the TDPs 1 and 2. After the pumps are destroyed the team heads for the west power plant door. This door is explosively breached; the team then heads to the diesel generator building where they explosively breach into that building and sabotage the most northern and then most southern generators. Alpha then proceeds back into the turbine building to retrace their steps back into the steam room where they destroy the prepositioned FLEX equipment here.

Bravo team waits 15 seconds after Alpha team moves north. Bravo team follows on Alpha teams' path until they reach the west power plant door. Here Bravo team heads south inside the turbine building, explosively breaching two doors until they gain access to the boiler room where they destroy the prepositioned FLEX equipment here.

Charlie team provides overwatch with the equipped M240 from the south side of the facility.

Scenario C DBT is the same as above except the Alpha and Bravo teams are both only three-man teams and Charlie team is removed.

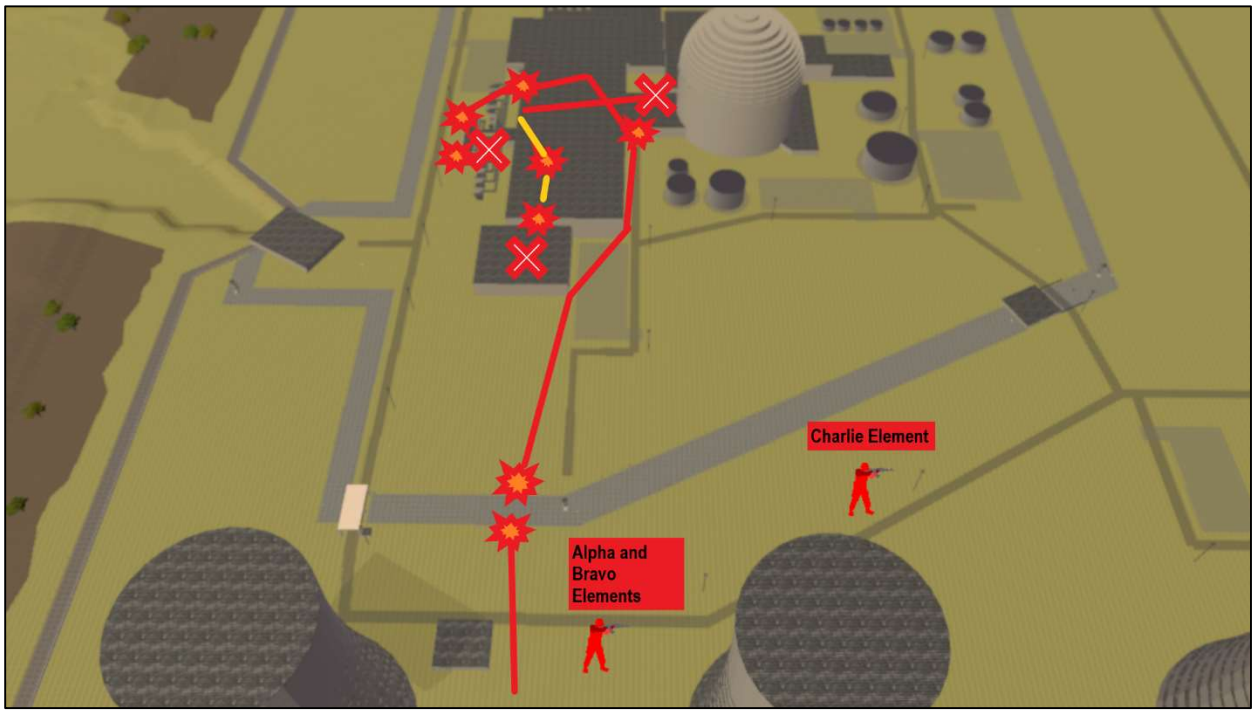


Figure A-3. Attack Scenario C.

4. Scenario D (Disrupt Power)

This attack scenario is pictured in Figure A-4. The adversaries are comprised of four elements: Alpha, a six-man team; Bravo, a six-man team; Charlie, a one-man team giving overwatch support; and Delta, a one-man team giving overwatch support.

Alpha and Bravo teams mechanically breach the PA fence in Sector 3. The teams then head west to the southern steam room door. Here they explosively breach door and move to the turbine building door, again explosively breaching. Alpha and Bravo disable TDPs 1 and 2. They then head to explosively breach the west power plant door. Next, they head to diesel generator building where they explosively breach into that building and sabotage the most northern and then most southern generators. Afterwards, Alpha and Bravo teams head back into the previously breached power plant door; here, Alpha and Bravo split. Alpha heads south to the boiler room. Alpha team breaches two doors to gain access to the boiler room where they destroy the prepositioned FLEX equipment. Bravo heads back into the steam room to destroy the prepositioned FLEX equipment there.

Charlie and Delta take positions on the southwest and southeast to provide overwatch with the equipped M240s.

Scenario D DBT is the same as above with the removal of Charlie and Delta elements and Alpha and Bravo are only three-man teams each.

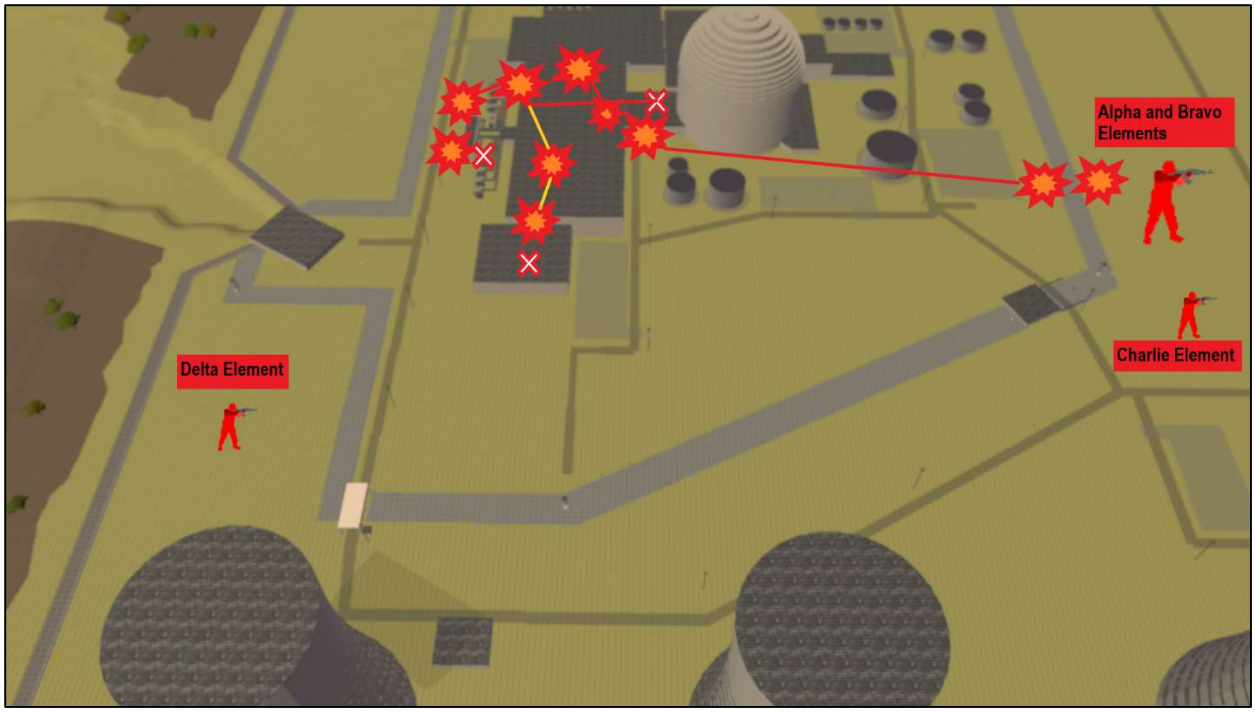


Figure A-4. Attack Scenario D.

Page intentionally left blank

Appendix B
EMRALD Model

Page intentionally left blank

Appendix B
EMRALD Model

Figure B-1 shows the C# scripts used to preprocess inputs to Simajin software, and the postprocess code used to save the data to a text file. These scripts are embedded in the *DoSimanij* action within the *RunSimanij* state.

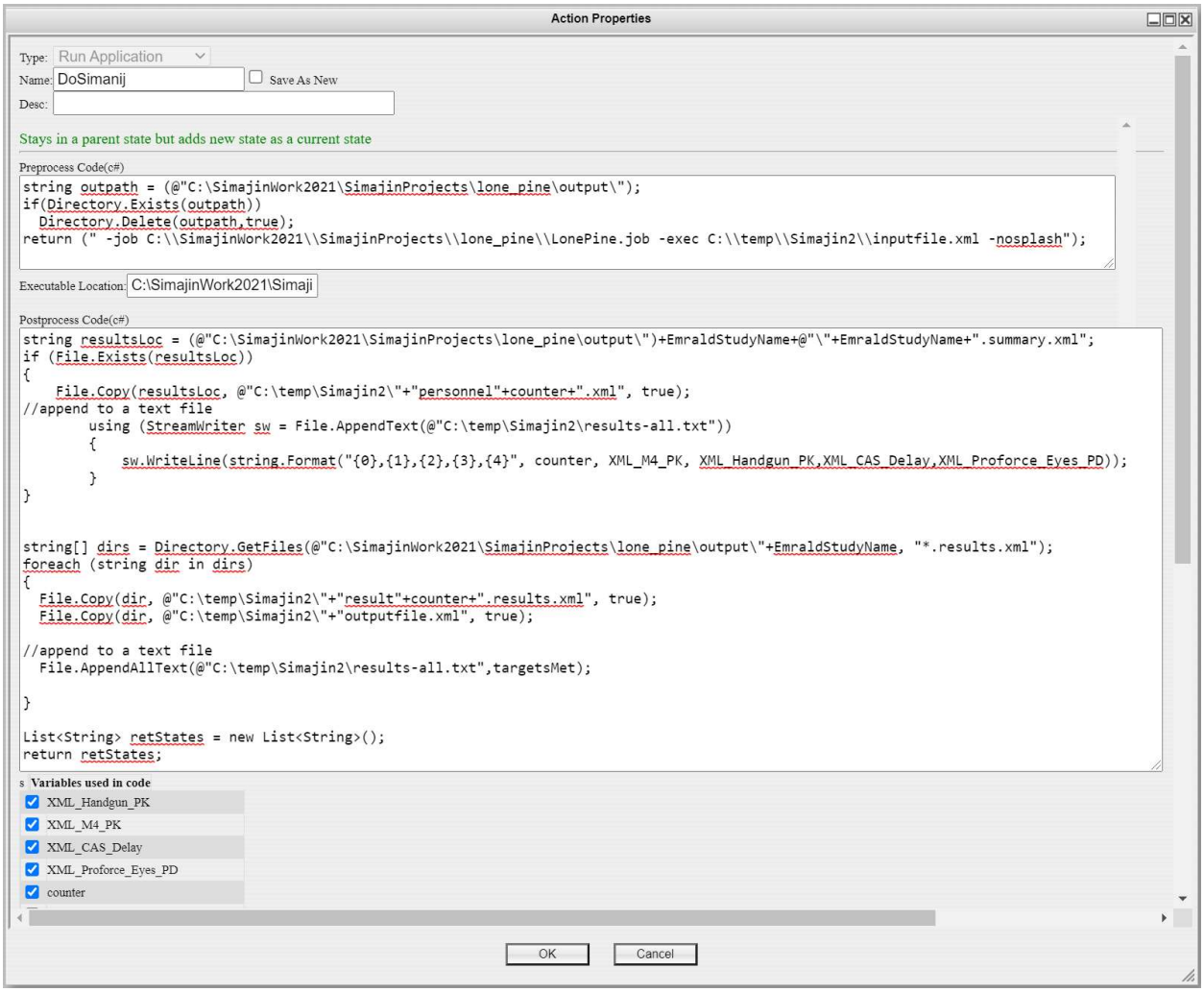


Figure B-1. *DoSimanij* action.

Figure B-2 shows the C# scripts used to read selected results from Simajin FOF simulations and saves them into a text file for further statistical analysis. This script is embedded in the *ReadResults* action within the *RunSimanij* state.

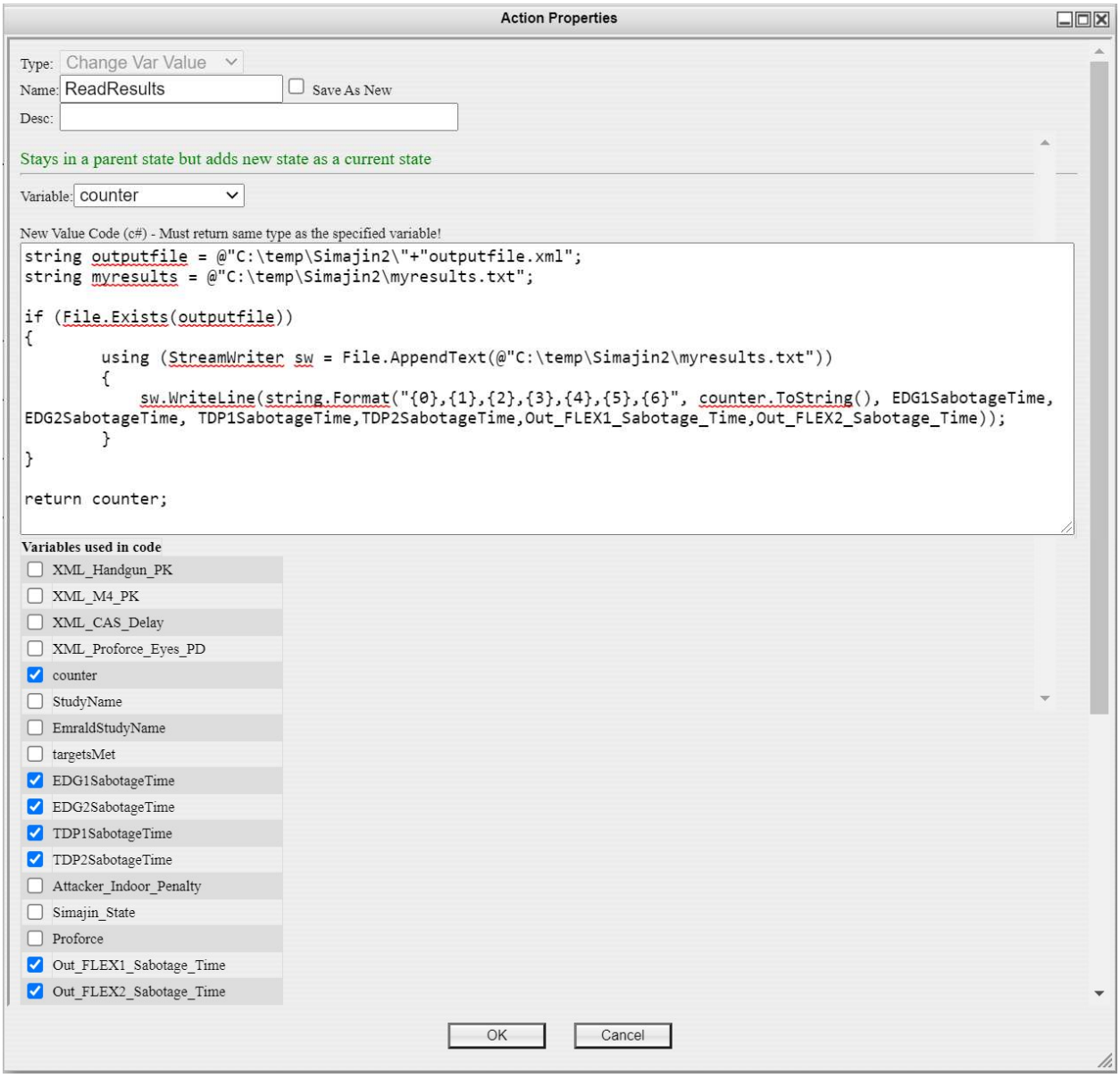


Figure B-2. *ReadResults* action.

Page intentionally left blank

Appendix C
Detailed Results

Page intentionally left blank

Appendix C
Detailed Results

1. Results for Scenario A:

a. With DBT attack and initial security posture (no guards reduction):

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	384	0.768	0.768 x 1E−6	0.768 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	0	0	0	0
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	36	0.072	0.072 x 4E−2	0.072 x 1.54E−4
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	77	0.154	0.154 x 1	0.154 x 1.83E−4
14	X	X	O	X	0	0	0 x 1	
15	X	X	X	O	2	0.004	0.004 x 1	
16	X	X	X	X	1	0.002	0.002 x 1	
Total					500	1	0.1629	6E−3

b. With beyond-DBT attack and initial security posture (no guards reduction):

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	276	0.552	0.552 x 1E−6	0.552 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	0	0	0	0
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	62	0.124	0.124 x 4E−2	0.124 x 1.54E−4
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	142	0.284	0.284 x 1	0.284 x 1.83E−4
14	X	X	O	X	3	6E−3	0.060	
15	X	X	X	O	13	2.6E−2	0.260	
16	X	X	X	X	4	8E−3	0.008	
Total					500	1	0.329	0.0401

c. With beyond-DBT attack minus one guard:

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	263	0.526	0.536 x 1E−6	0.536 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	0	0	0	0
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	66	0.132	0.124 x 4E−2	0.124 x 1.54E−4
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	127	0.254	0.34 x 1	0.34 x 1.83E−4
14	X	X	O	X	2	4E−3	4E−3	
15	X	X	X	O	24	4.8E−2	4.8E−2	
16	X	X	X	X	18	3.6E−2	3.6E−2	
Total					500	1	0.3473	8.8E−2

d. Beyond-DBT minus two guards:

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	277	0.554	0.554 x 1E−6	0.554 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	0	0	0	0
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	64	0.128	0.128 x 4E−2	0.128 x 1.54E−4
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	110	0.22	0.22 x 1	0.22 x 1.83E−4
14	X	X	O	X	4	8E−3	8E−3	
15	X	X	X	O	28	5.6E−2	5.6E−2	
16	X	X	X	X	17	3.4E−2	3.4E−2	
Total					500	1	0.3231	9.81E−2

e. Beyond-DBT attack minus three guards:

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	288	0.576	0.576 x 1E−6	0.576 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	0	0	0	0
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	51	0.102	0.102 x 4E−2	0.102 x 1.54E−4
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	111	0.222	0.222 x 1	0.222 x 1.83E−4
14	X	X	O	X	2	4E−3	4E−3	
15	X	X	X	O	27	5.4E−2	5.4E−2	
16	X	X	X	X	20	4E−2	4E−2	
Total					500	1	0.3241	9.81E−2

f. Beyond-DBT attack minus four guards:

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	273	0.546	0.546 x 1E−6	0.546 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	0	0	0	0
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	43	8.6E−2	8.6E−2 x 4E−2	8.6E−2 x 1.54E−4
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	115	0.23	0.23 x 1	0.23 x 1.83E−4
14	X	X	O	X	6	1.2E−2	1.2E−2	
15	X	X	X	O	33	6.6E−2	6.6E−2	
16	X	X	X	X	30	6E−2	6E−2	
Total					500	1	0.3714	0.1381

g. Beyond-DBT attack minus five guards:

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	274	0.5491	0.5491 x 1E−6	0.5491 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	0	0	0	0
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	19	0.0381	0.0381 x 4E−2	0.0381 x 1.54E−4
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	116	0.2325	0.2325 x 1	0.2325 x 1.83E−4
14	X	X	O	X	3	6E−3	6E−3	
15	X	X	X	O	47	9.42E−2	9.42E−2	
16	X	X	X	X	40	8E−2	8E−2	
Total					500	1	0.4143	0.1804

h. DBT attack minus four guards:

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	377	0.757	0.754 x 1E−6	0.754 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	0	0	0	0
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	39	7.8E−2	7.8E−2 x 4E−2	7.8E−2 x 1.54E−4
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	77	0.154	0.154 x 1	0.154 x 1.83E−4
14	X	X	O	X	1	2E−3	2E−3	
15	X	X	X	O	3	6E−3	6E−3	
16	X	X	X	X	1	2E−3	2E−3	
Total					500	1	0.1678	1E−2

2. Results for Attack Scenario B:

a. With DBT attack and initial security posture (no guards reduction):

No	Target A	Target B	FLEX Equipment	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	392	0.784	0.784 x 1E−6	
2	O	O	X	0	0	0	
3	O	X	O	15	0.03	0.03 x 1E−3	
4	O	X	X	0	0	0	
5	X	O	O	87	0.174	0.174 x 1E−3	
6	X	O	X	1	0.002	0.002 x 1E−3	
7	X	X	O	5	0.01	0.01 x 1	0.01 x 5E−4
8	X	X	X	0	0	0 x 1	
Total				500	1	1E−2	2E−4

b. Beyond-DBT attack with initial security posture:

No	Target A	Target B	FLEX Equipment	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	113	0.226	0.226 x 1E−6	
2	O	O	X	0	0	0	
3	O	X	O	39	0.78	0.78 x 1E−3	
4	O	X	X	0	0	0	
5	X	O	O	215	0.43	0.43 x 1E−3	
6	X	O	X	11	0.022	0.022 x 1E−3	
7	X	X	O	106	0.212	0.212 x 1	0.212 x 5E−4
8	X	X	X	16	0.032	0.032 x 1	
Total				500	1	0.2445	0.03326

c. Beyond-DBT attack minus one armed responder:

No	Target A	Target B	FLEX Equipment	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	99	0.198	0.198 x 1E−6	
2	O	O	X	0	0	0	
3	O	X	O	35	0.07	0.07 x 1E−3	
4	O	X	X	0	0	0	
5	X	O	O	226	0.452	0.452 x 1E−3	
6	X	O	X	17	0.034	0.034 x 1E−3	
7	X	X	O	97	0.194	0.194 x 1	0.194 x 5E−4
8	X	X	X	26	0.052	0.052 x 1	
Total				500	1	0.2466	5.27E−2

d. Beyond-DBT attack minus two armed responders:

No	Target A	Target B	FLEX Equipment	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	106	0.212	0.212 x 1E−6	
2	O	O	X	0	0	0	
3	O	X	O	32	0.064	0.064 x 1E−3	
4	O	X	X	2	4E−3	0	
5	X	O	O	208	0.416	0.416 x 1E−3	
6	X	O	X	11	2.2E−2	2.2E−2 x 1E−3	
7	X	X	O	100	0.2	0.2 x 1	0.2 x 5E−4
8	X	X	X	41	8.2E−2	8.2E−2 x 1	
Total				500	1	0.2825	8.26E−2

e. Beyond-DBT attack minus three armed responders:

No	Target A	Target B	FLEX Equipment	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	101	0.202	0.202 x 1E−6	
2	O	O	X	0	0	0	
3	O	X	O	35	0.07	0.07 x 1E−3	
4	O	X	X	0	0	0	
5	X	O	O	216	0.432	0.432 x 1E−3	
6	X	O	X	19	0.038	0.038 x 1E−3	
7	X	X	O	95	0.19	0.19 x 1	0.19 x 5E−4
8	X	X	X	34	0.068	0.068 x 1	
Total				500	1	0.2585	6.86E−2

f. Beyond-DBT attack minus four armed responders:

No	Target A	Target B	FLEX Equipment	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	102	0.204	0.204 x 1E−6	
2	O	O	X	0	0	0	
3	O	X	O	35	0.07	0.07 x 1E−3	
4	O	X	X	1	2E−3	0	
5	X	O	O	208	0.416	0.416 x 1E−3	
6	X	O	X	15	0.03	0.03 x 1E−3	
7	X	X	O	101	0.202	0.202 x 1	0.202 x 5E−4
8	X	X	X	38	0.076	0.076 x 1	
Total				500	1	0.2785	0.0766

g. Beyond-DBT attack minus five armed responders:

No	Target A	Target B	FLEX Equipment	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	84	0.168	0.168 x 1E−6	
2	O	O	X	0	0	0	
3	O	X	O	47	9.4E−2	9.4E−2 x 1E−3	
4	O	X	X	1	2E−3	0	
5	X	O	O	210	0.42	0.42 x 1E−3	
6	X	O	X	18	3.6E−2	3.6E−2 x 1E−3	
7	X	X	O	100	0.2	0.2 x 1	0.2 x 5E−4
8	X	X	X	40	8E−2	8E−2 x 1	
Total				500	1	0.2785	0.0766

h. DBT attack minus four armed responders:

No	Target A	Target B	FLEX Equipment	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	389	0.778	0.778 x 1E−6	
2	O	O	X	0	0	0	
3	O	X	O	31	0.062	0.062 x 1E−3	
4	O	X	X	0	0	0	
5	X	O	O	72	0.144	0.144 x 1E−3	
6	X	O	X	1	2E−3	2E−3 x 1E−3	
7	X	X	O	5	1E−2	1E−2 x 1	1E−2 x 5E−4
8	X	X	X	2	4E−3	4E−3 x 1	
Total				500	1	1.42E−2	4.2E−3

3. Results for Attack Scenario C:

a. With DBT attack and initial security posture (no guards reduction):

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	494	0.988	0.988 x 1E−6	0.988 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	5	1E−2	1E−2 x 4E−2	1E−2 x 1.54E−4
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	0	0	0	0
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	1	2E−3	2E−3 x 1	2E−3 x 1.83E−4
14	X	X	O	X	0	0	0	
15	X	X	X	O	0	0	0	
16	X	X	X	X	0	0	0	
Total					500	1	2.4E−3	2.9E−6

b. Beyond-DBT attack with initial security posture:

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	353	0.7	0.7 x 1E−6	0.7 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	102	0.2	0.2 x 4E−2	0.2 x 1.54E−4
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	0	0	0	0
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	7	1.4E−2	1.4E−2 x 1	1.4E−2 x 1.83E−4
14	X	X	O	X	9	1.8E−2	3.4E−2	
15	X	X	X	O	5	1E−2	3E−2	
16	X	X	X	X	24	4.8E−2	7.2E−2	
Total					500	1	9.8E−2	7.6E−2

c. Beyond-DBT attack minus one armed responder:

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	342	0.684	0.684 x 1E−6	0.684 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	101	0.202	0.202 x 4E−2	0.202 x 1.54E−4
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	0	0	0	0
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	21	0.042	0.042 x 1	0.042 x 1.83E−4
14	X	X	O	X	9	0.018	0.018	
15	X	X	X	O	5	0.01	0.01	
16	X	X	X	X	22	0.044	0.044	
Total					500	1	0.1221	0.0720

d. Beyond-DBT attack minus two armed responders:

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	291	0.582	0.582 x 1E−6	0.582 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	129	0.258	0.258 x 4E−2	0.258 x 1.54E−4
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	0	0	0	0
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	19	0.038	0.038 x 1	0.038 x 1.83E−4
14	X	X	O	X	14	0.028	0.028	
15	X	X	X	O	19	0.038	0.038	
16	X	X	X	X	28	0.056	0.056	
Total					500	1	0.1703	0.1220

e. Beyond-DBT attack minus three armed responders:

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	253	0.506	0.506 x 1E−6	0.506 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	148	0.296	0.296 x 4E−2	0.296 x 1.54E−4
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	0	0	0	0
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	21	4.2E−2	4.2E−2 x 1	4.2E−2 x 1.83E−4
14	X	X	O	X	21	4.2E−2	4.2E−2	
15	X	X	X	O	18	3.6E−2	3.6E−2	
16	X	X	X	X	39	7.8E−2	7.8E−2	
Total					500	1	0.2098	0.1561

f. Beyond-DBT attack minus four armed responders:

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	229	0.458	0.458 x 1E−6	0.458 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	149	0.298	0.298 x 4E−2	0.298 x 1.54E−4
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	0	0	0	0
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	26	5.2E−2	5.2E−2 x 1	5.2E−2 x 1.83E−4
14	X	X	O	X	27	5.4E−2	5.4E−2	
15	X	X	X	O	14	2.8E−2	2.8E−2	
16	X	X	X	X	55	0.11	0.11	
Total					500	1	0.2559	0.1921

g. Beyond-DBT attack minus five armed responders:

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	167	0.334	0.334 x 1E−6	0.334 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	176	0.352	0.352 x 4E−2	0.352 x 1.54E−4
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	0	0	0	0
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	27	5.4E−2	5.4E−2 x 1	5.4E−2 x 1.83E−4
14	X	X	O	X	48	9.6E−2	9.6E−2	
15	X	X	X	O	18	3.6E−2	3.6E−2	
16	X	X	X	X	64	0.128	0.128	
Total					500	1	0.3281	0.2601

h. DBT attack minus four armed responders:

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	480	0.96	0.96 x 1E−6	0.96 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	18	0.036	0.036 x 4E−2	0.036 x 1.54E−4
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	0	0	0	0
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	1	2E−3	2E−3 x 1	2E−3 x 1.83E−4
14	X	X	O	X	1	2E−3	2E−3	
15	X	X	X	O	0	0	0	
16	X	X	X	X	0	0	0	
Total					500	1	5.4E−3	2E−3

4. Results for Attack Scenario D:

a. With DBT attack and initial security posture (no guards reduction):

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	482	0.964	0.964 x 1E−6	0.964 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	16	0.032	0.032 x 4E−2	0.032 x 1.54E−4
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	0	0	0	0
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	2	4E−3	4E−3 x 1	4E−3 x 1.83E−4
14	X	X	O	X	0	0	0	
15	X	X	X	O	0	0	0	
16	X	X	X	X	0	0	0	
Total					500	1	5.3E−3	6.6E−6

b. Beyond-DBT attack with initial security posture:

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	215	0.43	0.43 x 1E−6	0.43 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	199	0.398	0.398 x 4E−2	0.398 x 1.54E−4
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	0	0	0	0
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	18	3.6E−2	0.036 x 1	0.036 x 1.83E−4
14	X	X	O	X	17	3.4E−2	3.4E−2	
15	X	X	X	O	15	3E−2	3E−2	
16	X	X	X	X	36	7.2E−2	7.2E−2	
Total					500	1	0.1879	0.1361

c. Beyond-DBT attack minus one armed responder:

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	202	0.4040	0.4 x 1E−6	0.4 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	193	0.3860	0.386 x 4E−2	0.386 x 1.54E−4
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	0	0	0	0
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	105	0.21	0.21 x 1	0.21 x 1.83E−4
14	X	X	O	X	0	0	0	
15	X	X	X	O	0	0	0	
16	X	X	X	X	0	0	0	
Total					500	1	0.2254	9.8E−5

d. Beyond-DBT attack minus two armed responders:

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	188	0.376	0.376 x 1E−6	0.376 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	196	0.392	0.392 x 4E−2	0.392 x 1.54E−4
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	0	0	0	0
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	26	5.2E−2	5.2E−2 x 1	5.2E−2 x 1.83E−4
14	X	X	O	X	27	5.4E−2	5.4E−2	
15	X	X	X	O	20	4E−2	4E−2	
16	X	X	X	X	43	8.6E−2	8.6E−2	
Total					500	1	0.2477	0.1801

e. Beyond-DBT attack minus three armed responders:

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	156	0.312	0.312 x 1E−6	0.312 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	191	0.382	0.382 x 4E−2	0.382 x 1.54E−4
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	0	0	0	0
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	28	5.6E−2	5.6E−2 x 1	5.6E−2 x 1.83E−4
14	X	X	O	X	24	4.8E−2	4.8E−2	
15	X	X	X	O	33	6.6E−2	6.6E−2	
16	X	X	X	X	68	0.136	0.136	
Total					500	1	0.3213	0.2501

f. Beyond-DBT attack minus four armed responders:

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	141	0.282	0.282 x 1E−6	0.282 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	170	0.34	0.34 x 4E−2	0.34 x 1.54E−4
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	0	0	0	0
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	38	7.6E−2	7.6E−2 x 1	7.6E−2 x 1.83E−4
14	X	X	O	X	38	7.6E−2	7.6E−2	
15	X	X	X	O	39	7.8E−2	7.8E−2	
16	X	X	X	X	74	0.148	0.148	
Total					500	1	0.3916	0.3021

g. Beyond-DBT attack minus five armed responders:

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	124	0.248	0.248 x 1E−6	0.248 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	153	0.306	0.306 x 4E−2	0.306 x 1.54E−4
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	0	0	0	0
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	25	5E−2	5E−2 x 1	5E−2 x 1.83E−4
14	X	X	O	X	29	5.8E−2	5.8E−2	
15	X	X	X	O	45	9E−2	9E−2	
16	X	X	X	X	124	0.248	0.248	
Total					500	1	0.4582	0.3961

h. DBT attack minus four armed responders:

No	EDG	TDP	FLEX DG	FLEX Pump	Number of events	FOF Probability	CCDP without FLEX	CCDP with FLEX
1	O	O	O	O	472	0.944	0.944 x 1E−6	0.944 x 1E−6
2	O	O	O	X	0	0	0	0
3	O	O	X	O	0	0	0	0
4	O	O	X	X	0	0	0	0
5	O	X	O	O	25	5E−2	5E−2 x 4E−2	5E−2 x 1.54E−4
6	O	X	O	X	0	0	0	0
7	O	X	X	O	0	0	0	0
8	O	X	X	X	0	0	0	0
9	X	O	O	O	0	0	0	0
10	X	O	O	X	0	0	0	0
11	X	O	X	O	0	0	0	0
12	X	O	X	X	0	0	0	0
13	X	X	O	O	2	4E−3	4E−3 x 1	4E−3 x 1.83E−4
14	X	X	O	X	0	0	0	
15	X	X	X	O	1	2E−3	2E−3	
16	X	X	X	X	0	0	0	
Total					500	1	8E−3	2E−3

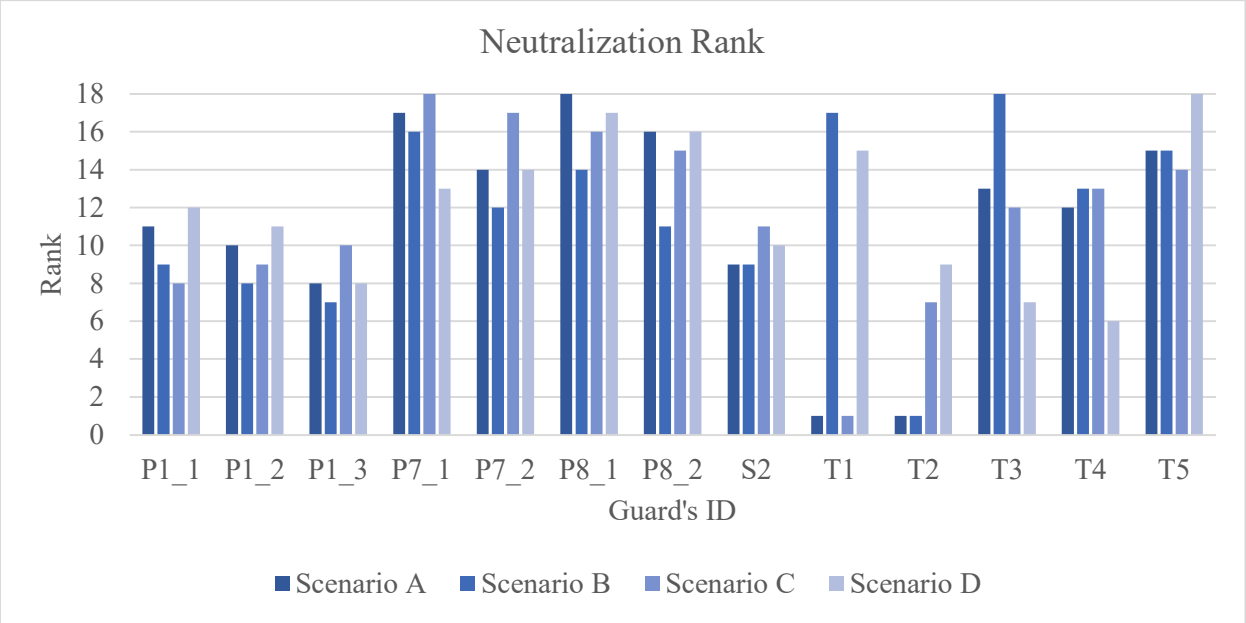
5. Results for weight-adjusted CCDP and the Importance Ranking for Armed Responders:

a. With DBT attack and initial security posture (no guards reduction):

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

b. Beyond-DBT attack with initial security posture:

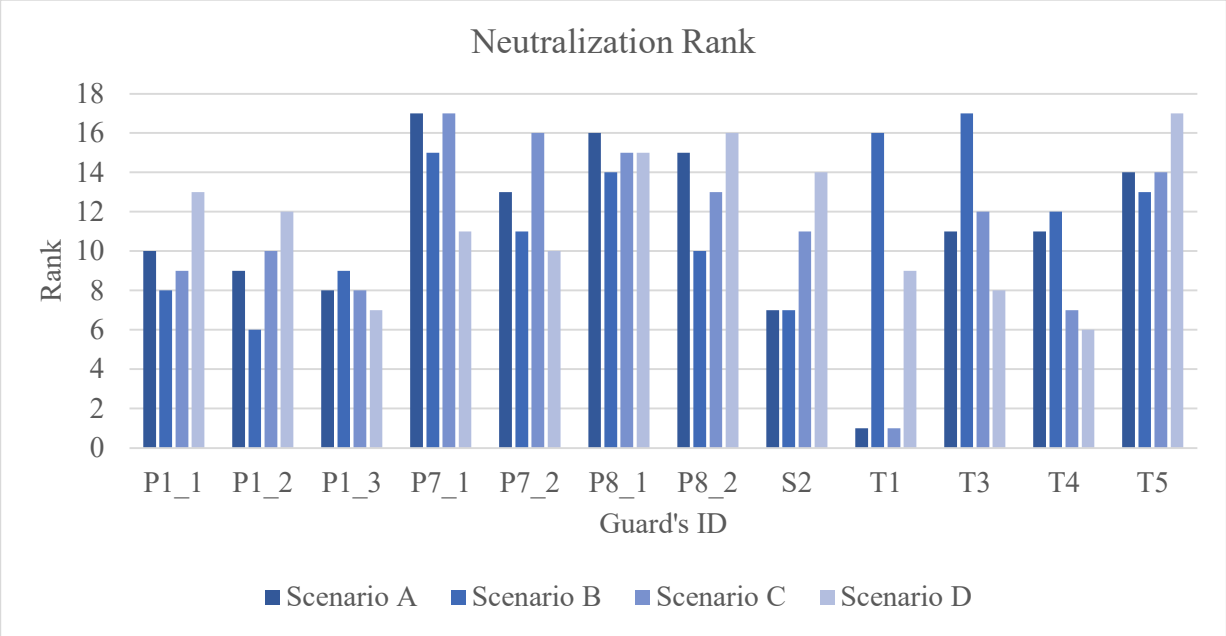
Scenario	CCDP	Importance Measure
Without FLEX Strategy		
Scenario A	3.29E−01	38.48%
Scenario B	2.45E−01	28.60%
Scenario C	9.80E−02	11.46%
Scenario D	1.84E−01	21.46%
Total	6.27E−01	100.00%
With FLEX Strategy		
Scenario A	4.00E−02	14.25%
Scenario B	3.26E−02	11.61%
Scenario C	7.60E−02	27.08%
Scenario D	1.32E−01	47.06%
Total	2.55E−01	100.00%



T2 was selected as the least effective responder.

c. Beyond-DBT attack minus one armed responder:

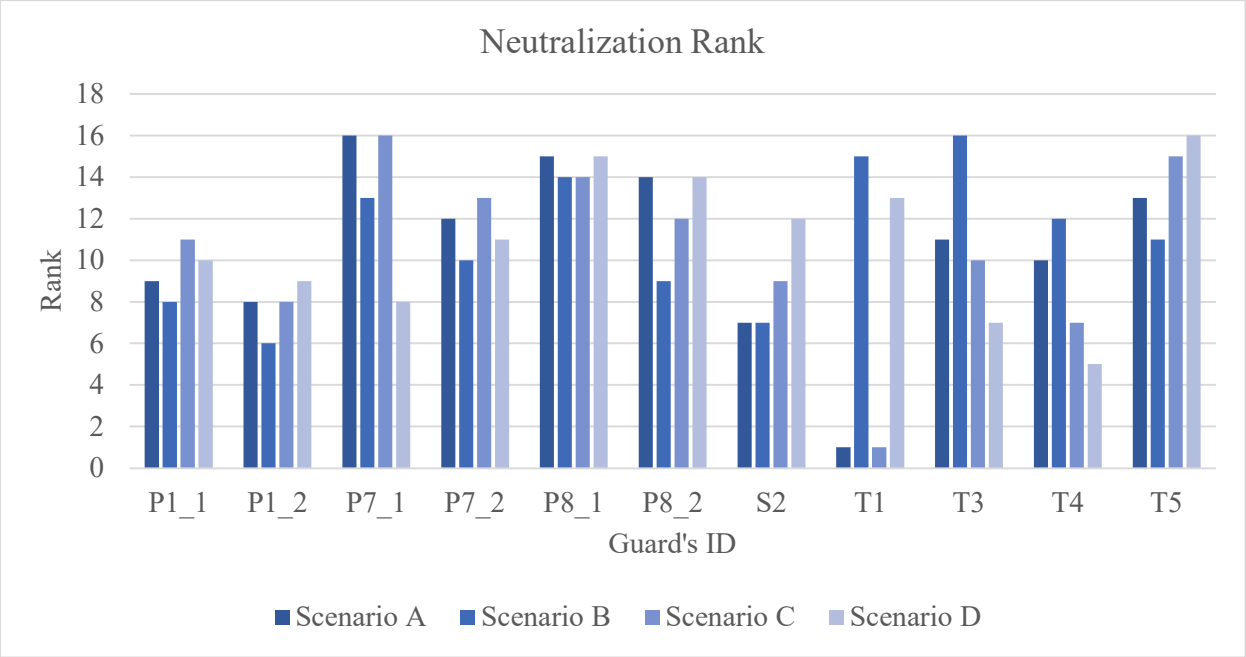
Scenario	CCDP	Importance Measure
Without FLEX Strategy		
Scenario A	3.45E−01	38.25%
Scenario B	2.47E−01	27.34%
Scenario C	1.22E−01	13.54%
Scenario D	1.88E−01	20.88%
Total	6.48E−01	100.00%
With FLEX Strategy		
Scenario A	8.20E−05	0.03%
Scenario B	5.27E−02	20.68%
Scenario C	7.00E−02	27.46%
Scenario D	1.32E−01	51.83%
Total	2.35E−01	100.00%



P1_3 was selected as the least effective responder.

d. Beyond-DBT attack minus two armed responders:

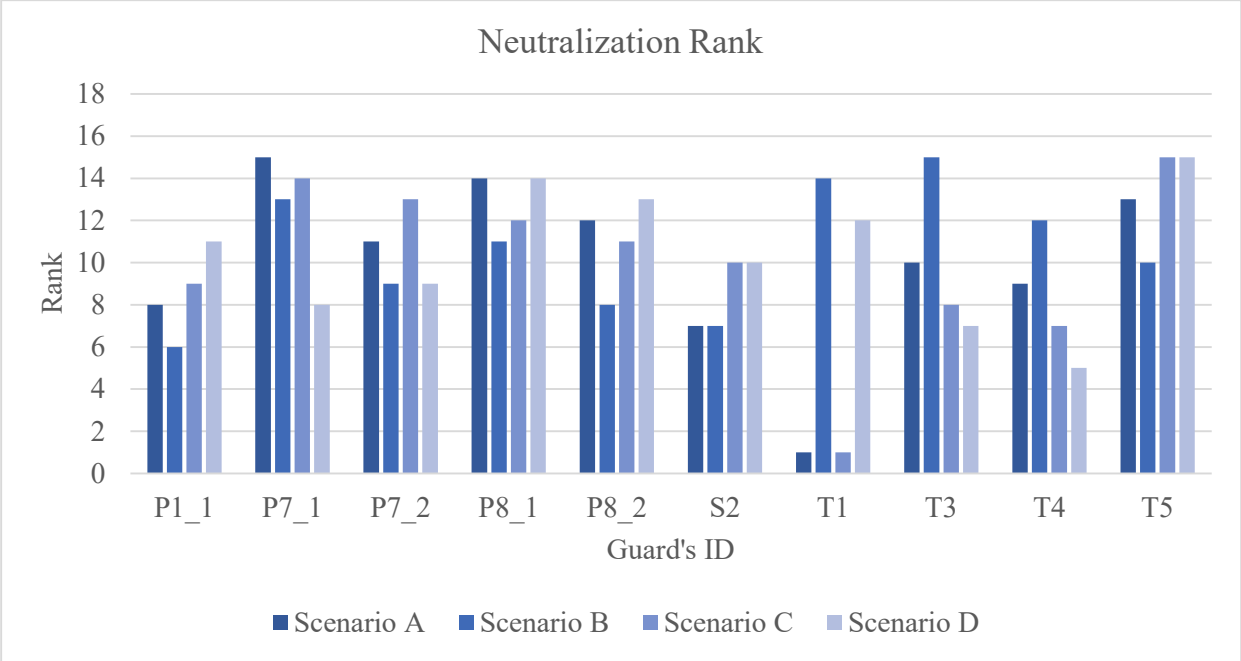
Scenario	CCDP	Importance Measure
Without FLEX Strategy		
Scenario A	3.23E−01	31.57%
Scenario B	2.83E−01	27.60%
Scenario C	1.70E−01	16.64%
Scenario D	2.48E−01	24.20%
Total	6.97E−01	100.00%
With FLEX Strategy		
Scenario A	9.81E−02	20.32%
Scenario B	8.26E−02	17.11%
Scenario C	1.22E−01	25.27%
Scenario D	1.80E−01	37.29%
Total	4.04E−01	100.00%



P1_2 was selected as the least effective responder.

e. Beyond-DBT attack minus three armed responders:

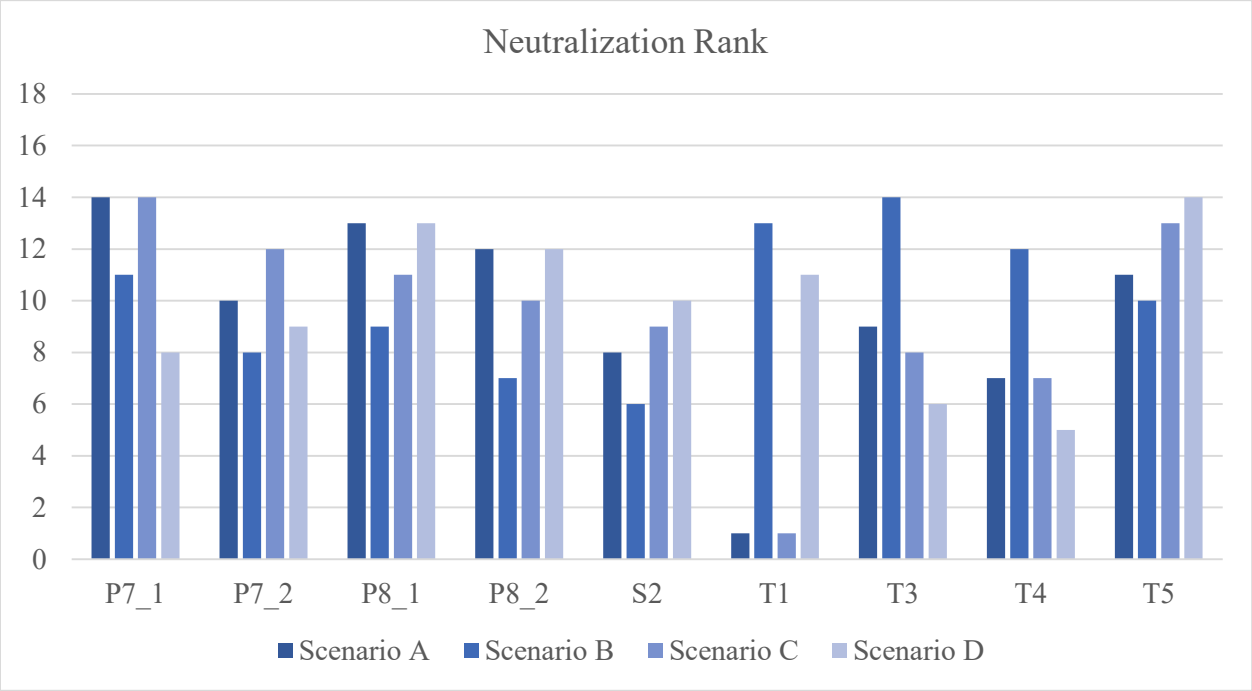
Scenario	CCDP	Importance Measure
Without FLEX Strategy		
Scenario A	3.24E−01	29.10%
Scenario B	2.59E−01	23.21%
Scenario C	2.10E−01	18.84%
Scenario D	3.21E−01	28.85%
Total	7.31E−01	100.00%
With FLEX Strategy		
Scenario A	9.81E−02	17.12%
Scenario B	6.86E−02	11.97%
Scenario C	1.56E−01	27.25%
Scenario D	2.50E−01	43.66%
Total	4.68E−01	100.00%



P1_1 was selected as the least effective responder.

f. Beyond-DBT attack minus four armed responders:

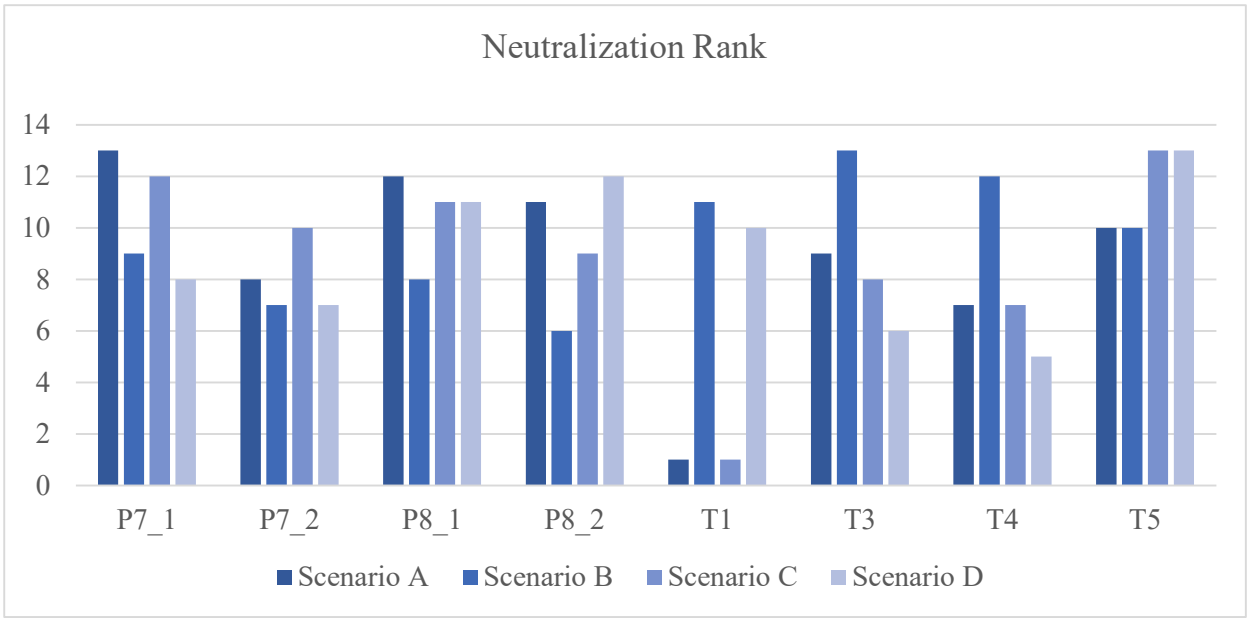
Scenario	CCDP	Importance Measure
Without FLEX Strategy		
Scenario A	3.71E−01	28.63%
Scenario B	2.79E−01	21.47%
Scenario C	2.56E−01	19.72%
Scenario D	3.92E−01	30.18%
Total	7.95E−01	100.00%
With FLEX Strategy		
Scenario A	1.38E−01	19.48%
Scenario B	7.66E−02	10.81%
Scenario C	1.92E−01	27.10%
Scenario D	3.02E−01	42.62%
Total	5.51E−01	100.00%



S2 was selected as the least effective responder.

g. Beyond-DBT attack minus five armed responders:

Scenario	CCDP	Importance Measure
Without FLEX Strategy		
Scenario A	4.14E−01	27.97%
Scenario B	2.81E−01	18.94%
Scenario C	3.28E−01	22.15%
Scenario D	4.58E−01	30.93%
Total	8.47E−01	100.00%
With FLEX Strategy		
Scenario A	1.80E−01	19.67%
Scenario B	8.07E−02	8.80%
Scenario C	2.60E−01	28.35%
Scenario D	3.96E−01	43.18%
Total	6.63E−01	100.00%



h. DBT attack minus four armed responders.

Scenario	CCDP	Importance Measure
Without FLEX Strategy		
Scenario A	1.68E−01	85.88%
Scenario B	1.42E−02	7.27%
Scenario C	5.40E−03	2.76%
Scenario D	8.00E−03	4.09%
Total	1.91E−01	100.00%
With FLEX Strategy		
Scenario A	1.01E−02	55.19%
Scenario B	4.20E−03	22.95%
Scenario C	2.00E−03	10.93%
Scenario D	2.00E−03	10.93%
Total	1.82E−02	100.00%