INL/EXT-20-59510
Revision 0

Light Water Reactor Sustainability Program

Integration of FLEX Equipment and Operator Actions in Plant Force-On-Force Models with Dynamic Risk Assessment

August 2020

U.S. Department of Energy

Office of Nuclear Energy

INL/EXT-20-59510
Revision 0

Integration of FLEX Equipment and Operator Actions in Plant Force-On-Force Models with Dynamic Risk Assessment

Robby Christian
Steven R. Prescott
Vaibhav Yadav
Shawn W. St Germain
John Weathersby

August 2020

http://www.LWRS.INL.Gov

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

ABSTRACT

The overall operation and maintenance cost to protect nuclear power plants accounts for approximately 7% of the total cost of power generation, with labor accounting for half of this cost. In the current research, from interaction with utilities and other stakeholders, it was determined that 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 presents a modeling and simulation framework for integrating Diverse and Flexible Mitigation Capability (FLEX) portable equipment performance with Force-on-Force models of a plant's physical security posture. The generic framework is described in detail, followed by a case study of modeling an adversarial attack aimed at causing a radiological release by sabotaging the plant's power supply and its ultimate heat sink capabilities at a hypothetical nuclear power plant. Two different FLEX deployment strategies, series and parallel, are modeled with distinct timelines. The results of the adversarial attack modeled in a commercial Force-on-Force tool are integrated with the FLEX deployment model in Idaho National Laboratory's (INL) dynamic modeling tool Event Modeling Risk Assessment using Linked Diagrams (EMRALD). Monte Carlo simulation is used to model the distribution of the timeline in FLEX deployment strategies. The results demonstrate that, even in the extreme case of a successful adversarial attack, deployment of FLEX equipment can result in a significantly high likelihood of preventing radiological release. The modeling and simulation framework 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.

CONTENTS

FIGURES

TABLES

ACRONYMS

ac	alternating current
AFW	auxiliary feedwater
CD	core damage
dc	direct current
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
FOF	force-on-force
IDS	intrusion detection system
INL	Idaho National Laboratory
LOOP	loss-of-offsite-power
LWRS	Light Water Reactor Sustainability
NPP	nuclear power plants
NRC	Nuclear Regulatory Commission
O&M	operation and management
PWR	pressurized-water reactor
SAFER	strategic alliance for FLEX emergency response
SBO	station blackout
SG	steam generator
TDP	turbine driven pump

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 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 have significantly lowered the price that 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 nuclear power plants with research to facilitate lowered O&M costs. Due to the use of nuclear materials, nuclear power plants have an additional cost burden in protecting fuel against theft or sabotage. The overall O&M cost to protect nuclear power plants 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 that 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.

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 excessive 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. nuclear power plants 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 that 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 that plant operators will take when an attack occurs to minimize the chance of core damage. It will take modeling and simulating of 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 that, when combined, provide a holistic approach to maintaining the effective security of the plant.
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" [5]. 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 [3]. 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 [4].

The nuclear industry needs to pursue an optimized plant security posture that considers efficiencies and innovative technologies to reduce costs while meeting security requirements. The use of 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 [6]. In this research, we focused on using one of the more complex simulation tools, ARES's AVERT [9] software, and evaluating what is needed to evaluate 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, Section 3 describes the integration of FLEX equipment with FOF modeling and simulation and presents a case study, followed by a conclusion in Section 4.

2. PHYSICAL SECURITY OPTIMIZATION

Physical security simulation software tools such as AVERT, Simajin, Scribe 3D, etc., can be used to model and simulate physical protection equipment, strategies, and plausible threat scenarios. These tools and models, and likely other analysis tools, can then be used to optimize many aspects of physical protection systems for nuclear power plants (NPPs) by incorporating additional strategies. This section describes a process for evaluating and optimizing the defense strategy for new technology, design/procedure changes, or including 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 the coupling of the FOF tool to additional simulation tools. This process consists of three main parts, base case evaluation, potential strategy evaluation, and staff optimization evaluation, and they are described in the following sections.

2.1 Base Case Evaluation

The first step is to determine baseline results from a plant's current defensive posture modeled in a simulation tool capable of capturing the strategies and procedures established by the NPP. Expert judgement, past FOF exercises, and possibly software tools are used to identify and order probable attack scenarios. Some software tools can even help determine likely attack paths for given targets. New models consisting of the defensive posture and the attack scenario can be constructed and run for each scenario until the contribution to the total defensive failure of the scenario drops below a certain level.

While in traditional numerical analysis there is only a single set of base results to compare against, FOF simulation analysis needs two different sets of data because of the high value of probability of effectiveness. If only the unmodified base case were used, relatively few failure scenarios or cases would be available to evaluate against, resulting in high uncertainty. To get results with low uncertainty, a results set needs to have a significant number of cases with varied paths of failure. If computing resources were unlimited, this could be accomplished by increasing the number of simulations runs; but given limited computing resources, it is accomplished through a reduction in the most effective areas of the defensive strategy or an increase in adversary force resources. These changes to overcome the more predominant defensive measures are used to construct a defense-in-depth (DID) model. While there are several ways, or model changes that can be used, to develop a DID model, the main purpose is to verify that one simple failure or change will not cause a significant reduction in the defensive posture. A couple of examples for constructing DID models are identifying and then removing the most effective guard post or increasing the adversary force beyond the design basis threat, followed by rerunning the FOF model and observing the change in effectiveness. While the DID should not drastically reduce the effectiveness,

the number of failed evaluation cases should significantly increase. 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 key is to capture the failure cases and the avenue of those failures from the simulation. If a certain DID model causes the same few avenues for failure as the original base case, other DID models need to be modeled or additional attack scenarios should be included to add additional failure paths. 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.

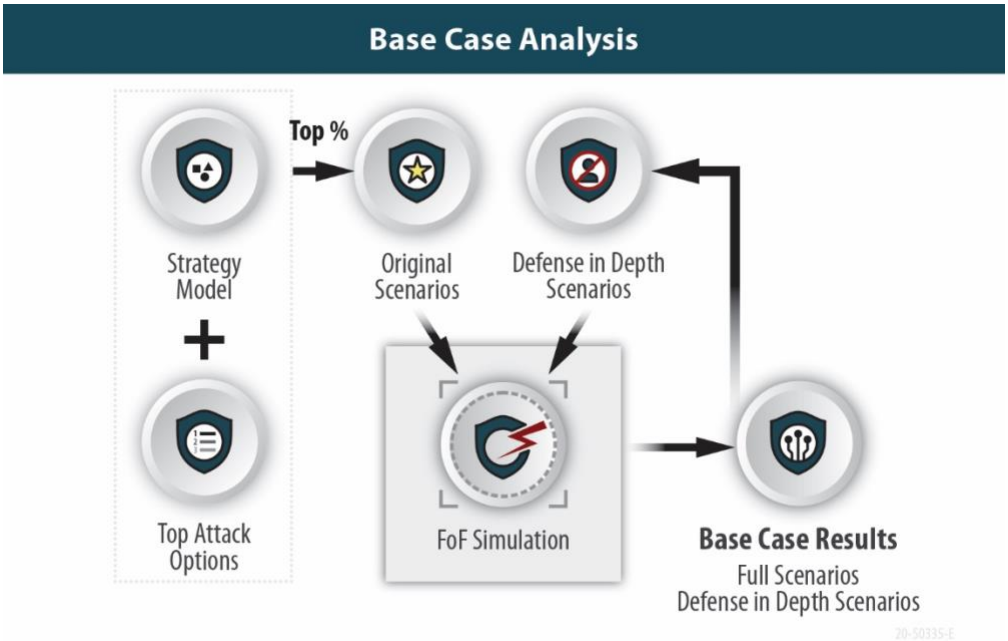


Figure 1. Flow for creating base case comparison results.

Many facilities currently have a previously evaluated defensive strategy model, and these can be used as a starting point to develop the comparison base cases. In summary, the process for developing the base case results are the following steps, as shown in Figure 1:

1. Model the plant protection strategy
2. Determine top attack options and model scenarios
3. Run FOF simulations and save results cases
4. Apply DID changes to scenarios
5. Run DID scenarios and save results cases.

2.2 Potential Strategy Evaluation

Each facility can have different options they consider for 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 to evaluate a potential change is having a tool that can correctly simulate the response or effect of the 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 that is designed for beyond-design external events as additional safety equipment after an attack. Other strategies could 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 behavior.

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

Once the change to be evaluated 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.

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.

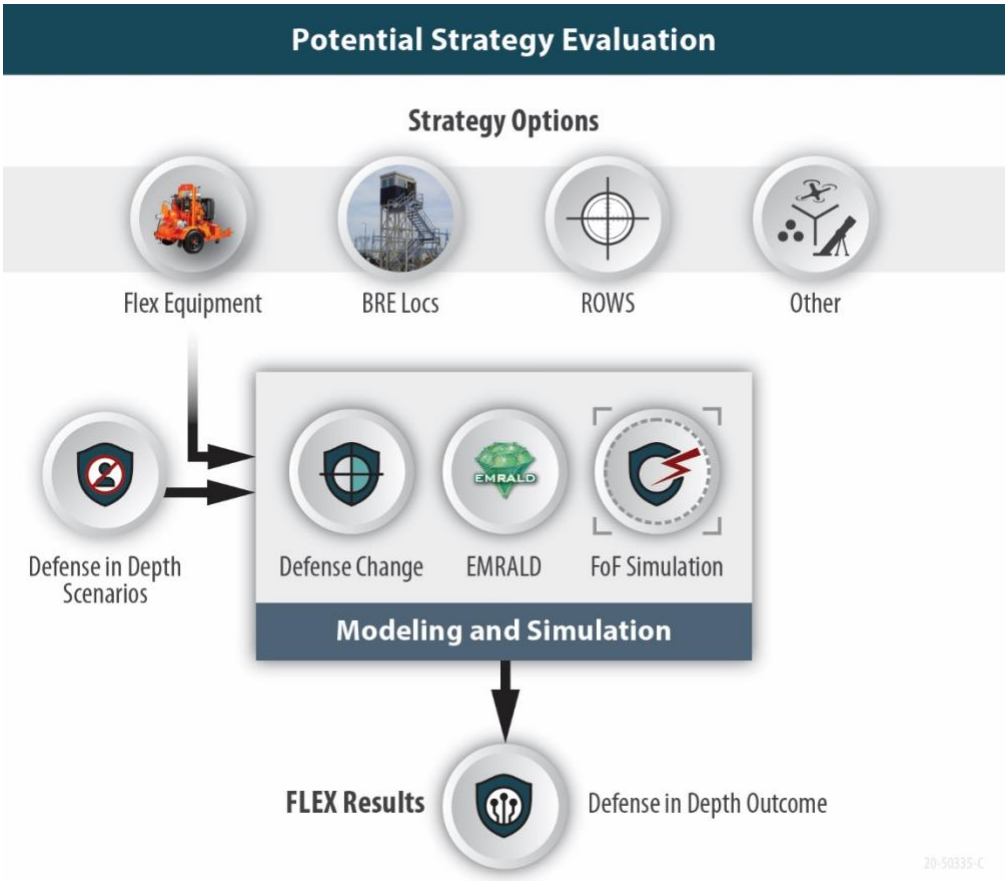


Figure 2. Flow for option evaluation.

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 that even after a potential staff reduction, an equivalent protective strategy is maintained, at least at its current level. The four main steps to this process are outlined in Figure 3 and described in the steps below. Before the process begins, a copy of the original and DID base case simulation scenarios and results is made. This is an iterative process and stops once the criteria has been met.

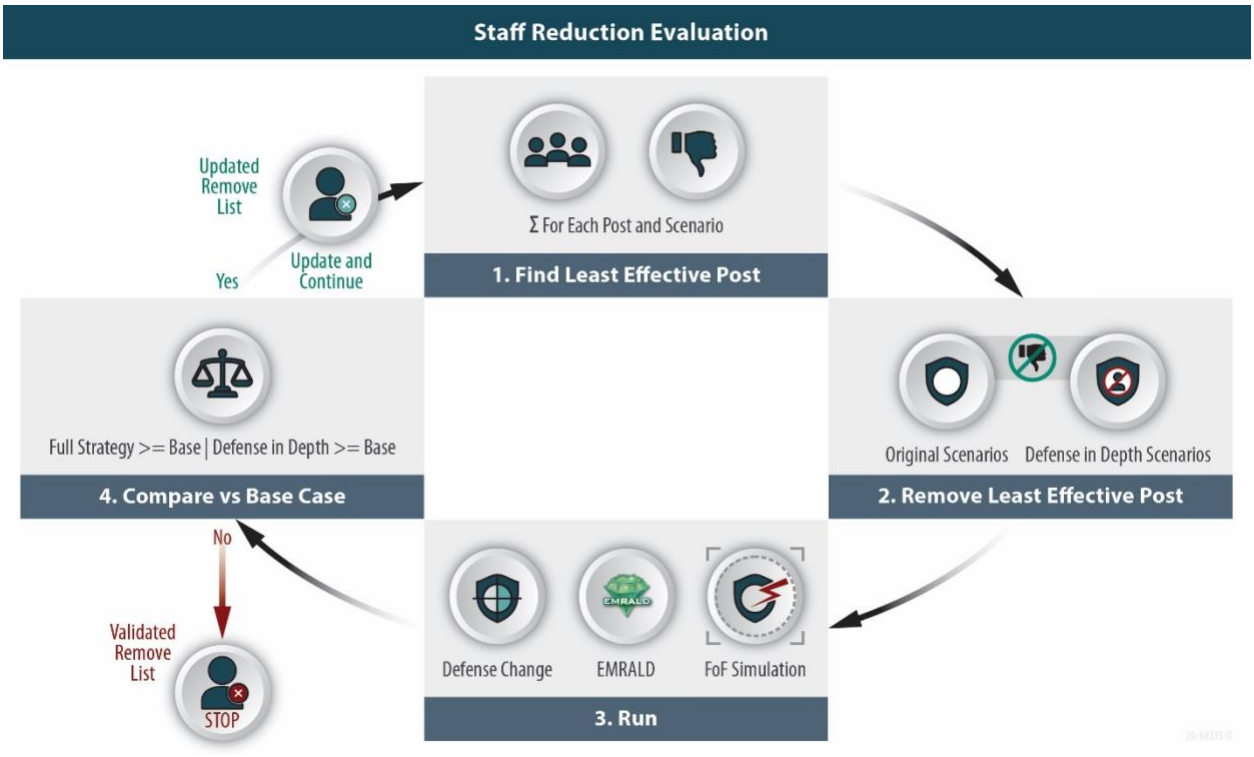


Figure 3. Process to evaluate staff reduction for a strategy change.

1. Use the current results to determine which post was the least effective for each scenario. The criteria for "least effective" should relate to no or noneffective engagement events, delay times, or identifying of intrusions. This evaluation can be done through a simple scoring process for each position and then each position is ordered accordingly.
2. Remove the identified "least effective" post from the scenarios and changed strategy model.
3. Run the FOF simulation with the defense changes and post removed to determine the effectiveness of the new model.
4. Compare the changed strategy model results, including the removed posts, with the original and DID results.
    a. If the new results are better than or statistically equivalent to the original and DID results, add the removed post to the "remove list." Repeat from Step 1.
    b. If the results are worse than the original and DID results, stop the loop.

Once the process has stopped, the posts in the "validated remove list" can be eliminated if the new 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 guards could be less impactful than iteratively removing the worst, one at a time.

3. FOF-FLEX INTEGRATION

The current regulation on the physical protection of NPPs promulgates the requirements to prevent radiation exposure to the public through deliberate actions [5]. As such, the physical protection system is designed to prevent sabotage actions on specific combinations of targets, termed as target sets, that can cause the plant to undergo a catastrophic failure and release radioactive material into the environment. The protection measures are considered as failed when a target set is sabotaged. This approach provides a clear and simplified acceptance criterion to the protection system 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.

The aforementioned time-margin can be utilized to perform mitigation actions in order to prevent plant damage. This section describes how FLEX mitigation strategies 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, execution times may vary significantly for different plants and scenarios [7]. 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.

The overview of the dynamic framework of FOF and FLEX model integration is illustrated in Figure 4. 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, create a statistical distribution of the timeline of FLEX equipment being 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 continue its normal operation. 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 accomplished 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.

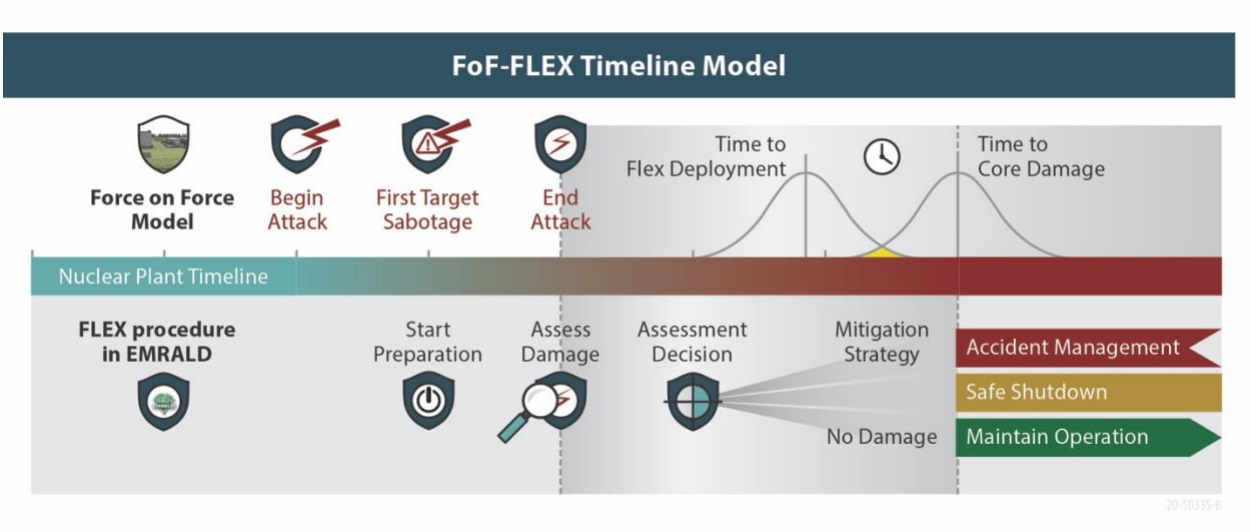


Figure 4. FOF-FLEX integration framework.

3.1 Case Study

A case study is described in this section to demonstrate the applicability of the FOF-FLEX integration model. A hypothetical attack scenario to 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 attack scenario, a group of adversaries attempts to cause a radiological release by sabotaging the 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 event tree for a PWR plant [10].

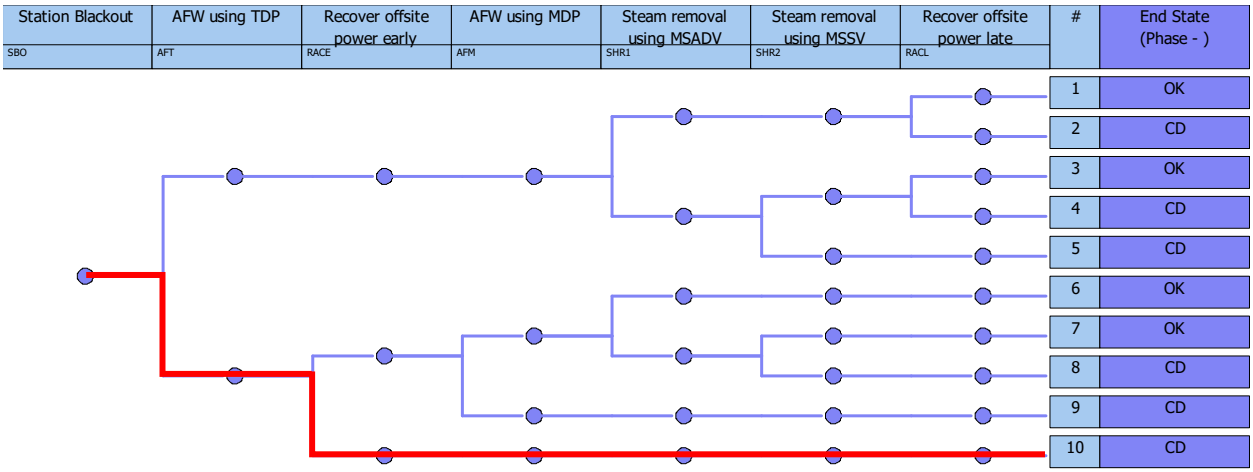


Figure 5. Sabotage scenario to inflict core damage.

Targets and the attack pathway to inflict the aforementioned core damage 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 a station blackout (SBO) event and damage the turbine driven pumps (TDPs) to disable the plant's passive heat removal capability. 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. If all of these targets are sabotaged, the nuclear plant will experience the core damage (CD) state within an hour [10].

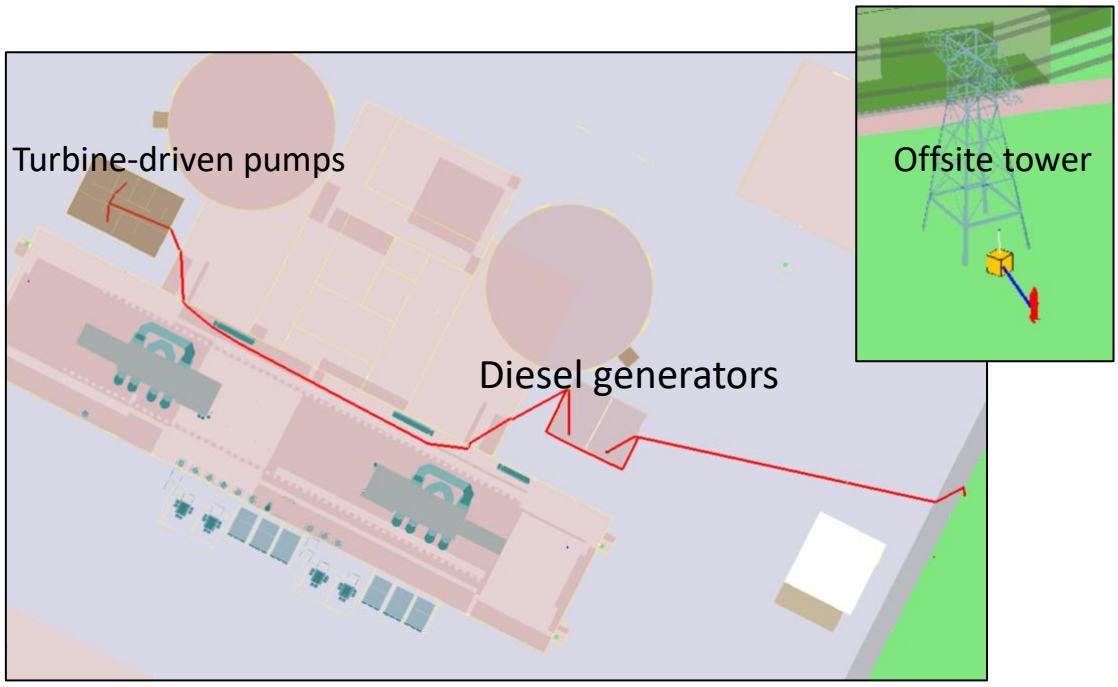


Figure 6. Attack targets and path in the force-on-force model.

A list of all possible outcomes from the attack scenario is shown in Table 1. If adversaries fail to sabotage any system in the target set, as indicated in the first outcome, the plant may continue its normal operation. Meanwhile, if the plant loses several of its safety functions without the initiation of safety-related events, as listed in Outcomes 2 through 4, the plant stops its operation in order to repair the damaged safety systems. If the initiating safety event occurs, it is mitigated with the design basis safety systems if they are available, as shown in Outcomes 5 and 6. Otherwise, the FLEX equipment are used to substitute the safety functions of the damaged design basis systems, as explained in Outcomes 7 and 8. FLEX Strategy A entails the use of FLEX equipment to provide the emergency power needed for the prolonged heat removal using TDPs. Meanwhile, FLEX Strategy B consists of utilizing the FLEX diesel generator to provide power and FLEX pumps to supply feedwater to the plant's secondary side. The time period to perform these FLEX strategies are taken from a reference study [10].

Table 1. Possible attack outcomes.

No.	System Availability			Mitigation Strategy
	Offsite Power	Emergency Diesel Generators (EDGs)	Turbine Driven Pumps (TDPs)	
1	✓	✓	✓	N/A (continue operation)
2	✓	✓	X	Non-transient shutdown
3	✓	X	✓	Non-transient shutdown
4	✓	X	X	Non-transient shutdown
5	X	✓	✓	Loss-of-offsite-power event tree
6	X	✓	X	Loss-of-offsite-power event tree
7	X	X	✓	FLEX Strategy A within 11 hours
8	X	X	X	FLEX Strategy B within 1 hour

3.1.1 Sequential FLEX Implementation

The procedure to implement a FLEX strategy in this case study is shown in Table 2. 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 FLEX Preparation" step in Figure 4. After the FOF simulation is completed, an assessment is done to determine the plant condition. Based on this assessment, the appropriate FLEX strategy is performed, following the execution actions in Table 2.

Table 2. 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 makeup pumps' hose	Preparation
5	Establish configuration to support FLEX 480V ac installation	Execution
6	Connect FLEX cables to 480V 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 diesel generator 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

The dynamic framework in Figure 4 is modeled in EMRALD, as shown in Figure 7. The process begins in the "Start" state, where variables in the model are initialized to their default values. Then, the model proceeds to the "Read_Avert" state, in which it runs the preconfigured FOF model built into the commercial AVERT platform and fetches the results from that simulation. The model proceeds to the "Plant_Continue_Operation" state if there is no damage to any components within the target set. Meanwhile, at the time when the first component is sabotaged, the model continues to the "FLEX_Preparation" state.

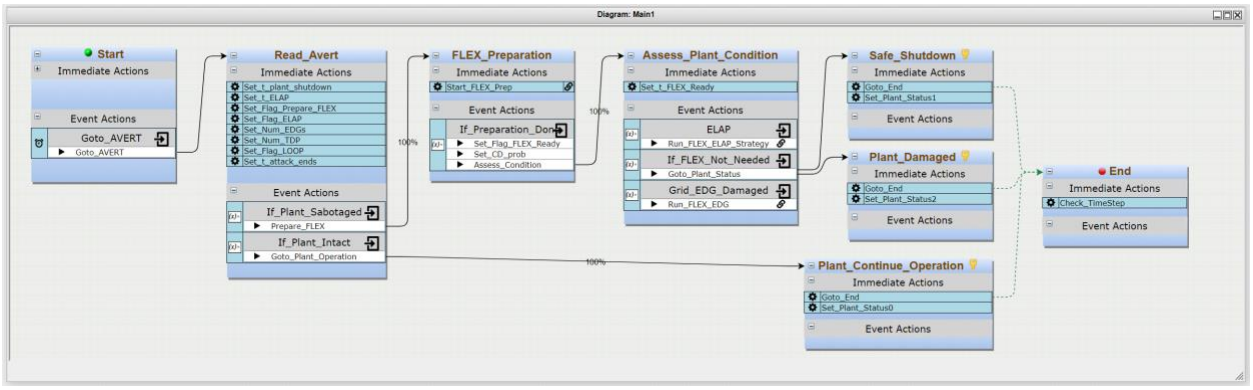


Figure 7. Main diagram of EMRALD model.

The immediate action named "Start_FLEX_Prep" within the "FLEX_Preparation" state transfers the simulation to the "Keys_and_doors" state in an EMRALD subdiagram shown in Figure 8. This subdiagram details the preparation of FLEX equipment, as shown in Table 2, which includes aligning the makeup pumps, starting the FLEX diesel generators (DGs) and connecting the electrical cables. Uncertainties on the completion time of actions shown in this subdiagram were modeled following a normal distribution. Upon starting the FLEX DGs, there is a statistical probability for the DGs to fail-t-start and to fail to continuously run. If any of those failures happen, the simulation transitions to the "FLEX_DG_Status" state in which a repair action is performed. Uncertainties in the timing to repair DGs and the success probability are modeled in EMRALD. After all the preparation actions are completed, the event action "Set_Flag_FLEX_Ready" triggers the "If_Preparation_Done" event in the main diagram shown in Figure 7.

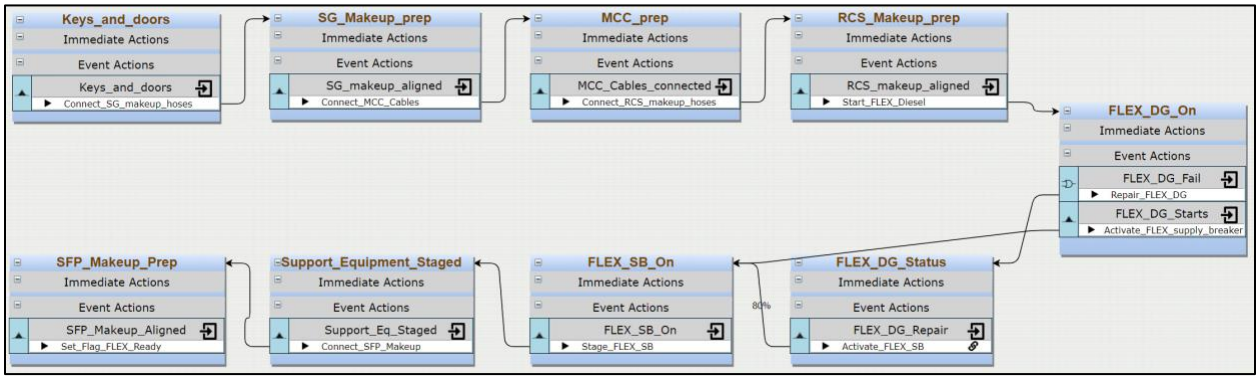


Figure 8. Sequential preparation of FLEX equipment.

The component failure diagram for FLEX DGs are shown in Figure 9. Initially, the component is in the "FLEX_DG_Standby" state while it is not in use. When the EMRALD simulation enters the "FLEX_DG_On" state in Figure 8, it triggers the "FLEX_DG_Demand" in Figure 9. The component's failure to start up on demand is represented by the arrow leading to the "FLEX_DG_Fail" state with a probability of 1E-2. The "FLEX_DG_Active" state is active if the component starts successfully. The "FLEX_DG_FR" event contains the component failure rate and the required mission time data, which is set as 24 hours in this case study. Any fail-to-run event within this mission time triggers the "FLEX_DG_Fail" state. If both FLEX DGs are in this state, the "FLEX_DG_Fail" event in Figure 8 is activated. This event leads to an attempt to repair the FLEX DGs with a success probability of 0.8. This repair will cause the simulation to switch from the "FLEX_DG_Fail" state to the "FLEX_DG_Active" state.

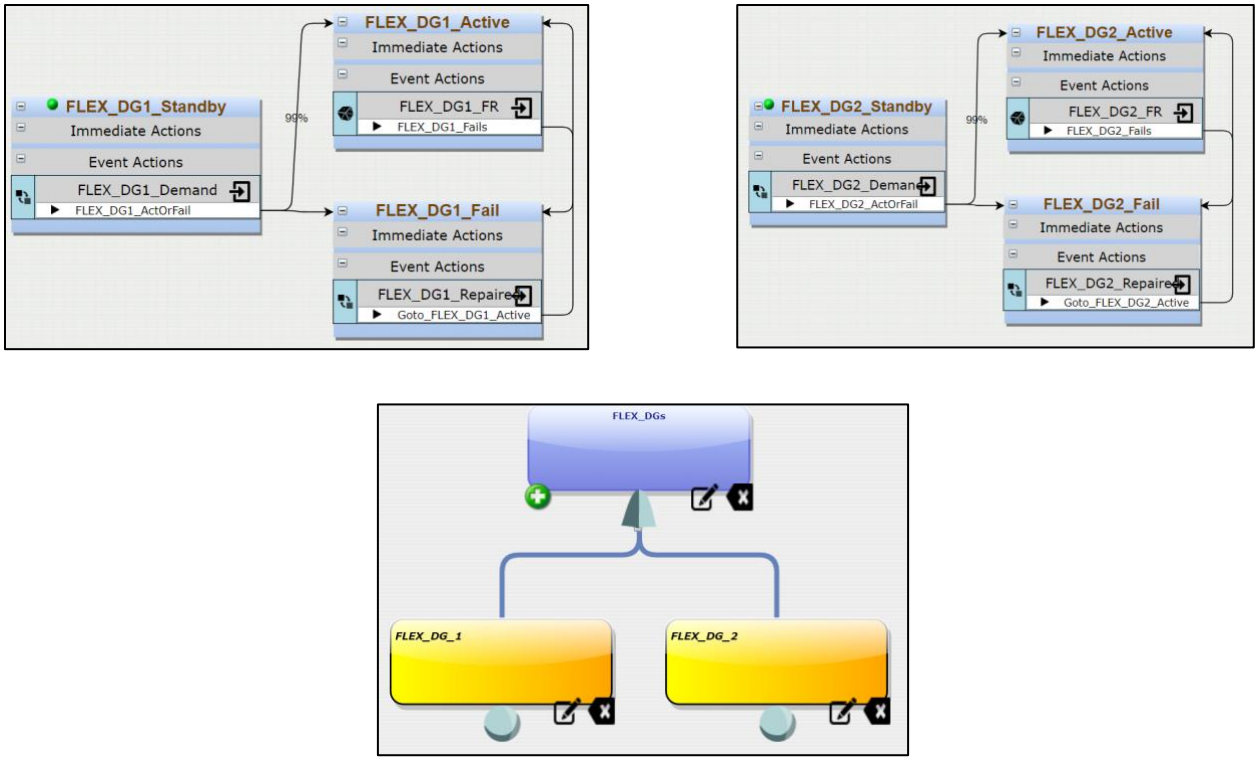


Figure 9. FLEX DG failure model.

The diagram for the failure of FLEX auxiliary feedwater (AFW) pumps is shown in Figure 10. This model is similar to the failure model for the FLEX DGs. However, repair actions are not included for FLEX AFW pumps for simplification. Furthermore, the failure rate for FLEX AFW pumps are also adjusted accordingly for pumps.

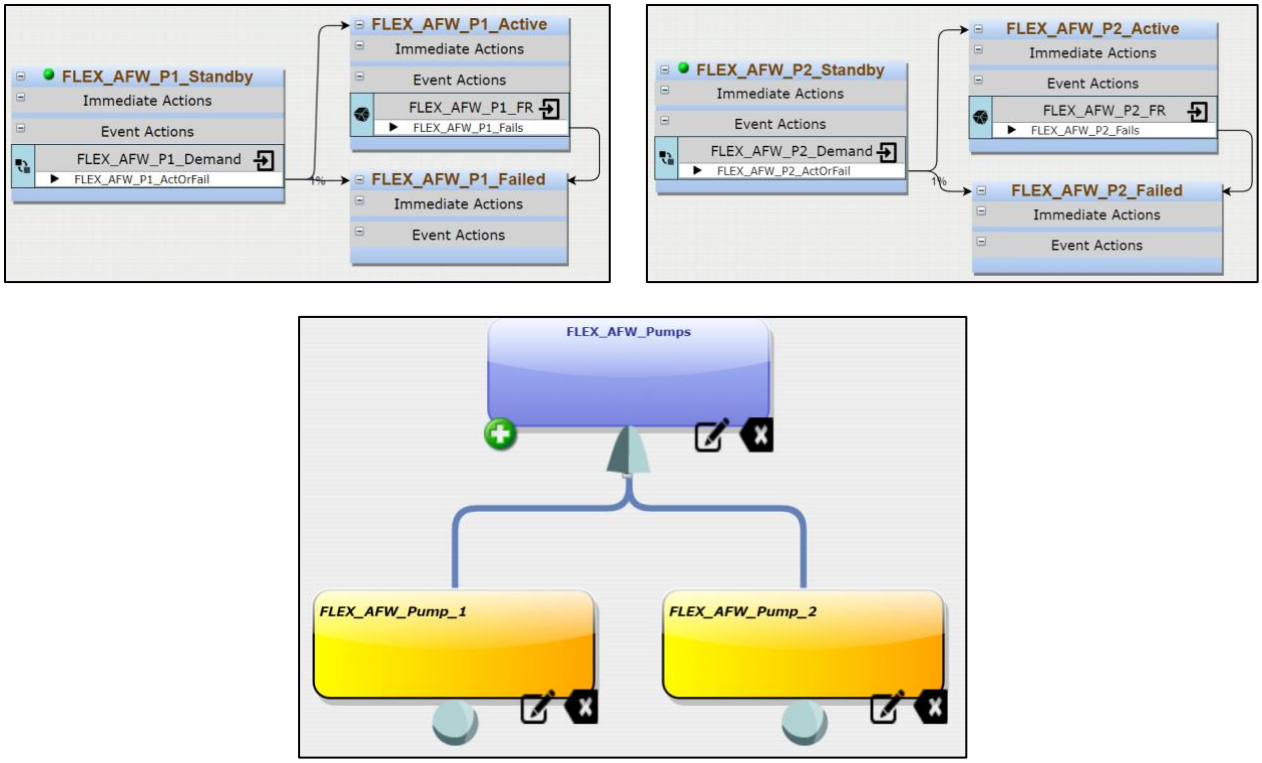


Figure 10. FLEX pump failure model.

Figure 11 shows the EMRALD model of the execution of FLEX strategy. The starting "Check_FLEX" state is actuated from the "Assess_Plant_Condition" state in Figure 7. It is followed with actions to execute the FLEX strategy, which include direct current (dc) load shedding, opening the electrical breakers, aligning the steam generator (SG) pumps, performing the pump transfer switch, and maintaining the FLEX strategy for 24 hours. The time distribution on each action is modeled in each event. The end "FLEX_ELAP_Strategy" state checks if the FLEX components run successfully for the entire mission time of 24 hours and ends the simulation with the "Safe_Shutdown" state if they do.

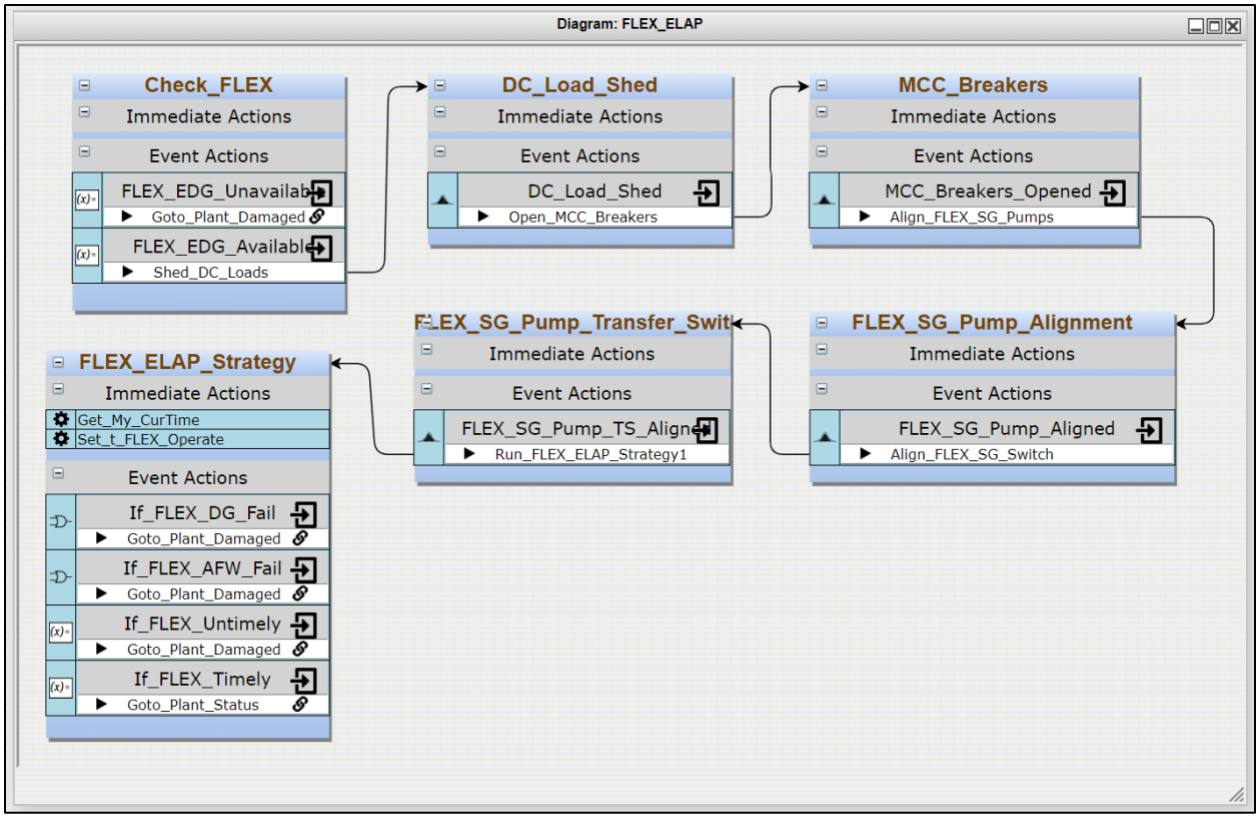


Figure 11. Sequential execution of FLEX strategy.

3.1.2 Parallel FLEX Implementation

The previous section presented the EMRALD model when actions in the FLEX strategy are performed sequentially. However, several of the FLEX actions, such as preparations of pumps and electrical components, can be done in parallel. Parallel implementation of FLEX actions may reduce the equipment preparation time before the reactor is damaged, potentially increasing the success likelihood of the FLEX strategy. In order to analyze the benefits of a parallel FLEX implementation, we modeled the FLEX preparation actions in EMRALD, as shown in Figure 12. In this subdiagram, the preparation steps for the electrical system are done simultaneously with the steps to prepare pump connections. This parallel action is made possible by the "Connect_MCC_Cables" action in the "SG_Makeup_Prep" state. The sequence from the "MCC_prep" state to the "FLEX_SB_On" state is simulated in parallel with the sequence of the "SG_Makeup_prep" state to the "SFP_Makeup_Prep" state. The simulation control is returned to the main diagram in Figure 7 upon reaching the "Support_Equipment_Staged" state.

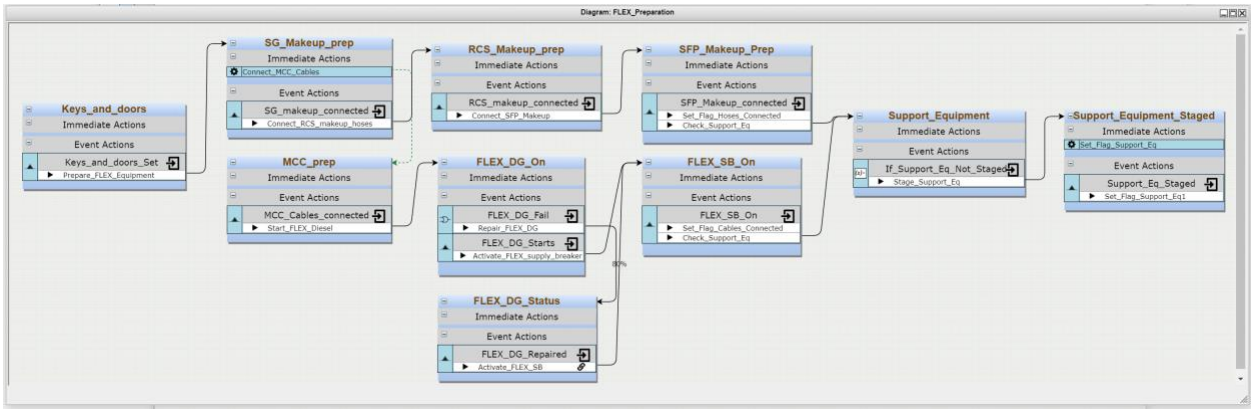


Figure 12. Parallel preparation of FLEX equipment.

The execution of FLEX strategy to provide alternating current (ac) power in case EDGs are sabotaged is shown in Figure 13. The process starts with a conditional check to ensure that the FLEX DGs are available before performing the dc load shedding and opening the electrical breakers. The "FLEX_EDG_Running" state models the FLEX DG probabilistic fail-to-start event and the failure to continuously run event as previously described. The simulation activates the "Plant_Damage" state when FLEX strategy is performed too late or when there are random failures of FLEX equipment within the required mission time.

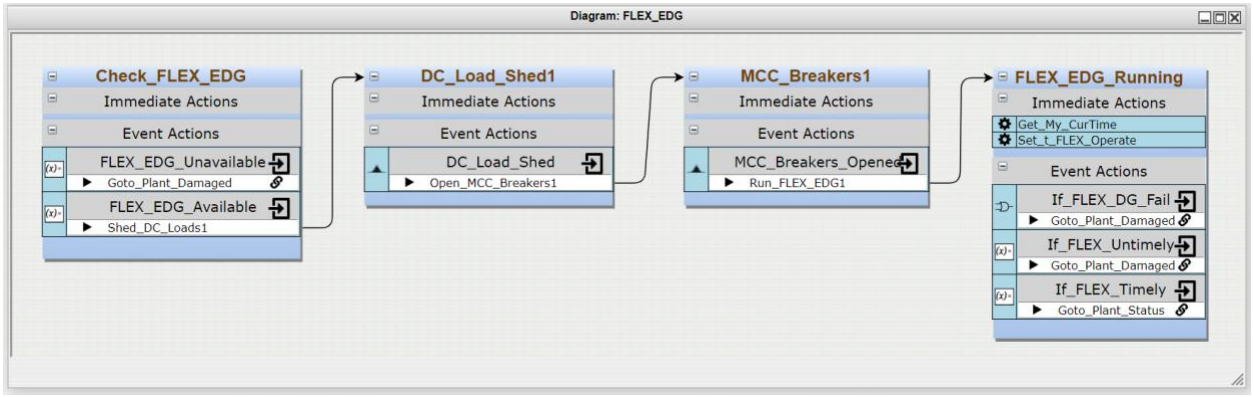


Figure 13. FLEX EDG strategy.

In the event where all components within the target set are sabotaged, the FLEX extended loss-of-ac-power (ELAP) strategy is executed following Figure 14. The subdiagram starts with conditional events to check whether FLEX DGs are still running prior to shedding the dc load and opening the breakers. These actions are done simultaneously with the alignment of the FLEX SG makeup pumps. Upon the completion of these two states, the "When_FLEX_ELAP_Ready" event is activated. Probabilistic events of random failures of FLEX equipment are modeled in the "If_FLEX_DG_Fail" and "If_FLEX_AFW_Fail" events.

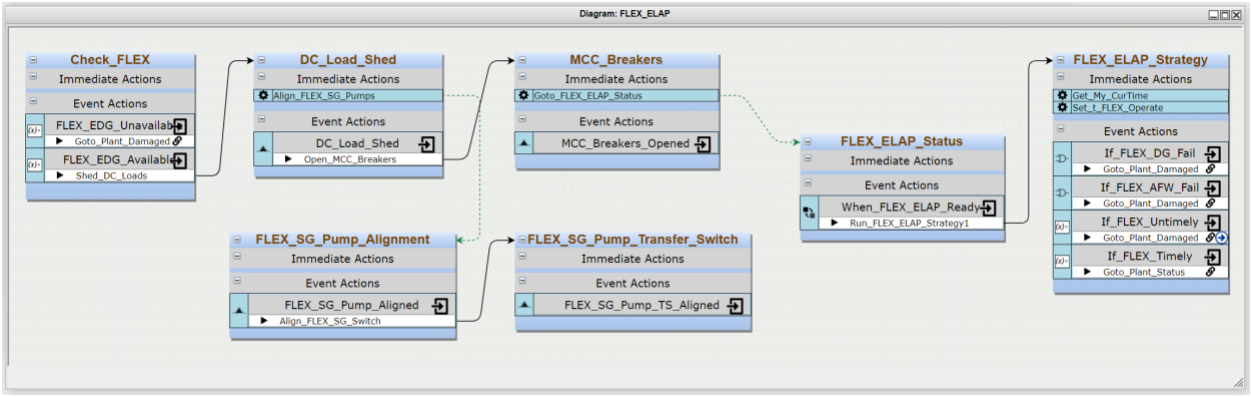
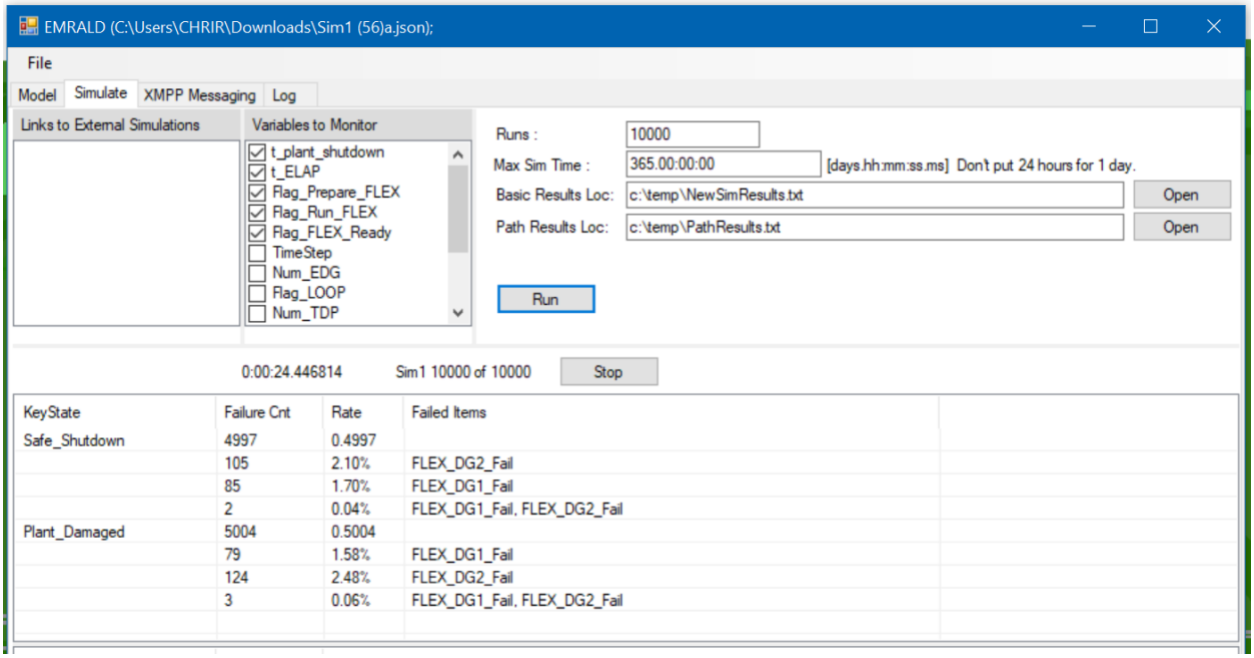


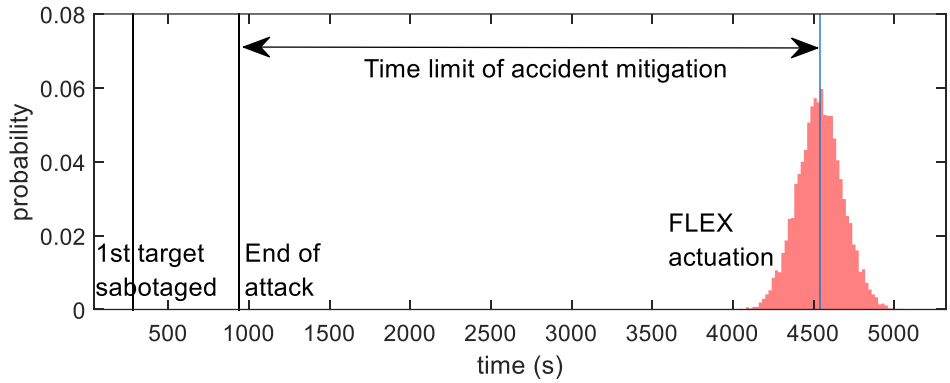
Figure 14. FLEX ELAP strategy.

3.2 Results and Discussion

The EMRALD model explained in the previous section was saved as a text input file and was solved using the EMRALD solver. The solver is a separate standalone software that runs the input file with a Monte Carlo sampling technique and tallies the number of key states encountered by each simulation. The solver window for the sequential FLEX actions is shown in Figure 15(a). It ran the model using ten thousand random instances and showed that it has a nearly 50% probability of reaching a safe shutdown state. Further details are shown in the form of a timeline in Figure 15(b). It shows the distribution of the FLEX actuation timing. Without the FLEX strategy, this particular FOF scenario would have resulted in a radiological release event. However, by using the FLEX mitigation strategy, there is about a 50% probability that such an event could be prevented in a timely manner. This result shows that FLEX can be utilized to mitigate the adverse effect of sabotage-induced events.



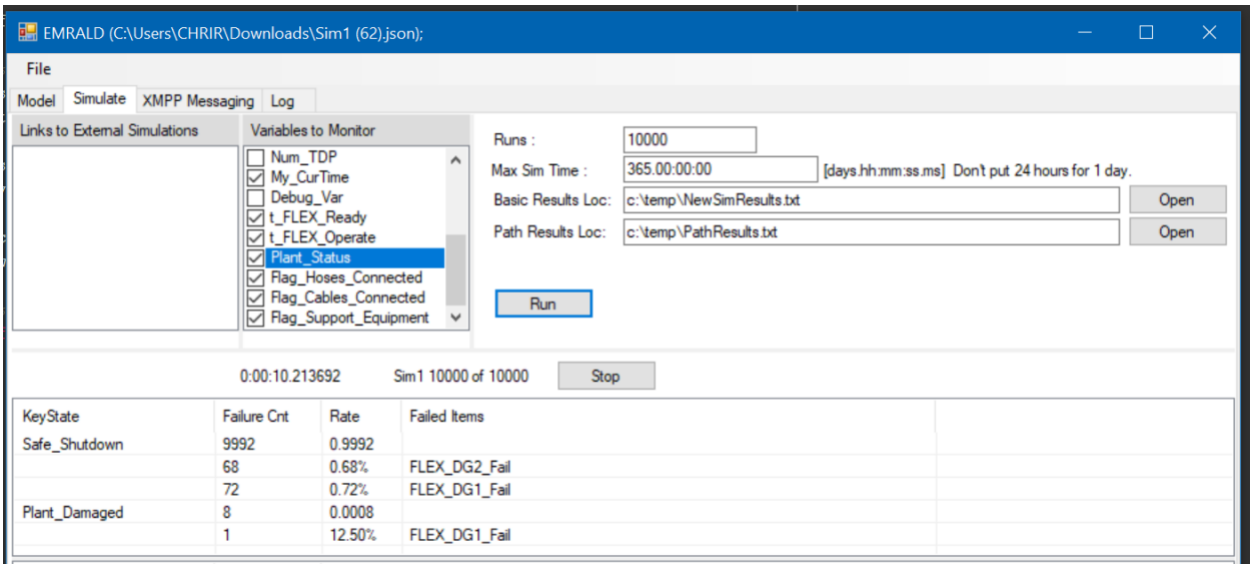
(a) EMRALD Results



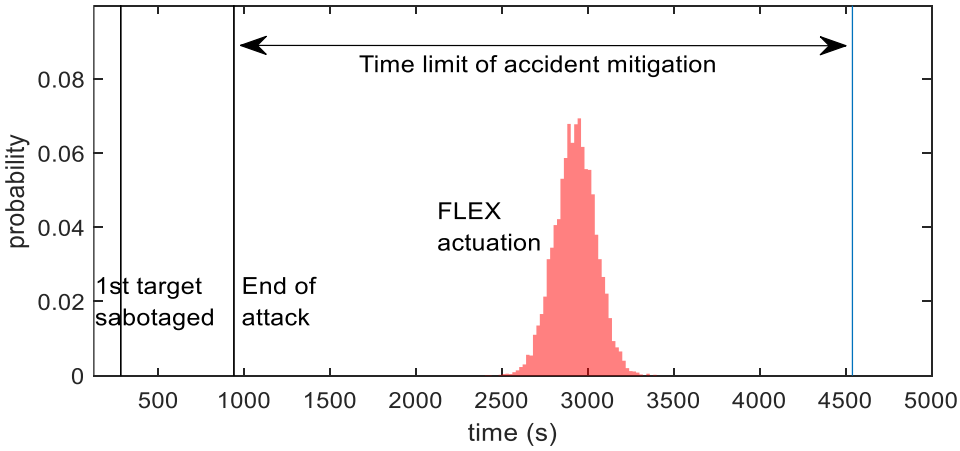
(b) Timeline Evaluation

Figure 15. Results of sequential FLEX actions.

Although the results from the sequential FLEX model show the benefit of the FLEX strategy in physical security, it can be improved further by reducing the time required to prepare the FLEX equipment. For that reason, we investigated the EMRALD model on the parallel FLEX actions as well. Results from this model are shown in Figure 16. The figure indicates that a parallel execution of the FLEX mitigation actions could shorten the actuation timing such that the success probability of the FLEX strategy was increased considerably. The small chance of plant damage of 8E-4 might be caused by random failures of the FLEX equipment.



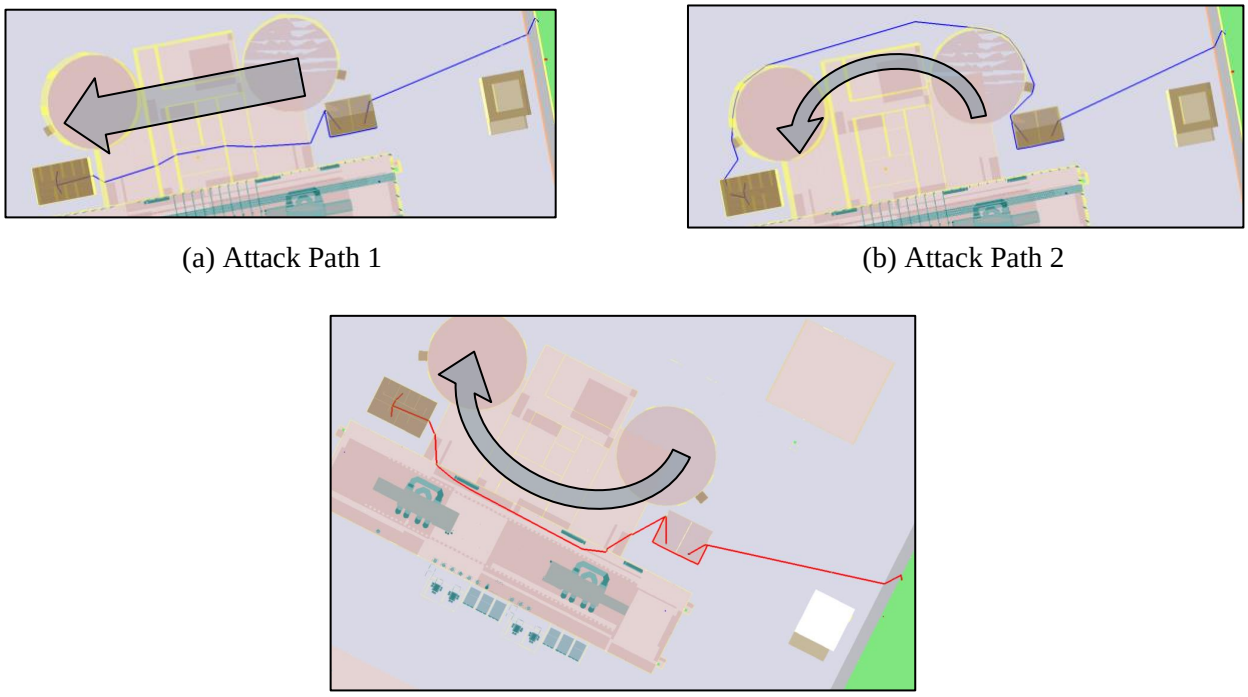
(a) EMRALD Results



(b) Timeline Evaluation

Figure 16. Results of the parallel FLEX actions model.

The results shown in Figure 15 and Figure 16 were obtained from a single FOF simulation such that there are discrete time points when the first target was sabotaged, when the attack ended, and the time limit to actuate the FLEX strategy. In practice, there are uncertainties within the FOF analysis that originate from the adversary exact attack path, the IDS, the adversary and response force's timing, and the adversary neutralization event. In order to capture these uncertainties, the FOF simulation was repeated multiple times. Three adversary attack paths of the shortest-distance and two detour paths were evaluated, as shown in Figure 17. For each of these paths, 100 Monte Carlo runs were simulated, resulting in a total of 300 simulations.



(a) Attack Path 1

(b) Attack Path 2

(c) Attack Path 3

Figure 17. Attack paths for the FOF scenario.

The outcome of the 300 FOF simulations are tabulated in the "Probability" column of Table 3. As given in the Table, there were several outcomes with zero probability. Outcome 1 through 4 were not observed due to the facts that the electric tower is located offsite and, therefore, it is not protected. Meanwhile, Outcome 6 did not occur because the TDPs are located further inside the plant complex compared to EDGs, such that there were no cases in which adversaries disabled TDPs but not EDGs. The probability of CD without a FLEX strategy was calculated by multiplying the sabotage event probability with probability of the design basis system failures obtained from a generic probabilistic risk assessment model. For example, the CD probability for Outcome 5 was obtained from the product of 0.843 and the conditional CD probability of a LOOP event, which was taken as 1E-3 in this case. Meanwhile, the conditional CD probability for Outcome 8 is 1, as shown in Figure 5. Each of the FOF simulation results were imported into EMRALD to evaluate the success likelihood of FLEX strategies. Ten thousand Monte Carlo runs were simulated for each of these FOF results, totaling to three million simulations. The resulting CD probabilities are tabulated in the last column of Table 3. It was found that a FLEX mitigation strategy could significantly reduce the likelihood for a CD and radiological release into the environment due to sabotage attacks by a factor of three. Although the model and data used in this case study are hypothetical, it still serves as a proof of concept for the proposed FOF-FLEX integration and how existing resources in NPPs can be incorporated into the physical security evaluation to improve the plant's safety and security.

Table 3.Results from multiple FOF simulations.

No.	System Availability			Mitigation Strategy	Probability	Core Damage Probability Without FLEX	Core Damage Probability With FLEX
	Offsite Power	EDGs	TDPs				
1	✓	✓	✓	N/A (continue operation)	0	0	
2	✓	✓	X	Non-transient shutdown	0	0	
3	✓	X	✓	Non-transient shutdown	0	0	
4	✓	X	X	Non-transient shutdown	0	0	
5	X	✓	✓	Loss-of-offsite-power event tree	0.843	8.43E-4	
6	X	✓	X	Loss-of-offsite-power event tree	0	0	
7	X	X	✓	FLEX Strategy A within 11 hours	5.67E-2	2.27E-3	8.7E-6
8	X	X	X	FLEX Strategy B within 1 hour	0.1	0.1	1.83E-5
Total					1	0.1035	8.74E-4

4. CONCLUSION AND FUTURE WORK

This report presents a modeling and simulation framework for integrating FLEX portable equipment performance with FOF models of a plant's physical security posture. The generic framework is described in detail, followed by a case study modeling an adversarial attack aimed at causing a radiological release by sabotaging the plant's power supply and its ultimate heat sink capabilities at a hypothetical PWR. Two distinct FLEX deployment strategies, series and parallel, are modeled with distinct timelines. The results of the adversarial attack modeled in a commercial FOF tool, AVERT, are integrated with the FLEX deployment model in EMRALD. Monte Carlo simulation is used to model the distribution of the timeline in FLEX deployment strategies. The results demonstrate that, even in the extreme case of a successful adversarial attack, deployment of 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.

Ongoing and future efforts in this area include: 1) Integrate the FLEX-FOF model with a thermohydraulic model of FLEX equipment modeled in RELAP5 for an increased accuracy of timeline calculations; 2) Implement the framework on a plant's specific physical security posture and FLEX equipment; 3) Integrate with other commercial FOF tools, such as Simajin. The INL team has engaged with the vendor of Simajin, RhinoCore, for this integration; 4. Model the FLEX equipment and enclosure as a target set in the physical security posture.

5. REFERENCES

1. Pacific Gas & Electric Company, "PG&E Company 2018 Nuclear Decommissioning Costs Triennial Proceeding Prepared Testimony – Volume 1," December 13, 2018. https://analysis.nuclearenergyinsider.com/pge-seeks-decommissioning-head-start-cost-estimates-rise.
2. NRC. 2012. *Issuance of Order to Modify Licenses with Regard to Requirements for Mitigation Strategies for Beyond-Design-Basis External Events*, EA-12-049, Washington, D.C: U.S. NRC.
3. United States Nuclear Regulatory Commission. "Emergency Preparedness in Response to Terrorism." https://www.nrc.gov/about-nrc/emerg-preparedness/about-emerg-preparedness/response-terrorism.html#one.
4. United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73. "Physical Protection of Plants and Materials." https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/.
5. United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73, Section 55. "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage." https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0055.html.
6. Garcia, Mary Lynn. 2005. *Vulnerability Assessment of Physical Protection Systems*. Elsevier.
7. Nuclear Energy Institute. 2017. "Guidance for Optimizing the Use of Portable Equipment," NEI 16-08, Washington D.C.
8. Idaho National Laboratory. "Event Modeling Risk Assessment using Linked Diagrams (EMRALD)." https://emrald.inl.gov/SitePages/Overview.aspx.
9. 2020. "AVERT Physical Security." Ares Security Corp. https://aressecuritycorp.com/avert.
10. Kang, D., & Chang, S. 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 vol. 275*, 142–153.
11. Nuclear Energy Institute. 2016. "NEI 12-06 Rev. 4: Diverse and Flexible Coping Strategies (FLEX) Implementation Guide." Washington, D.C.: NEI.