INL/RPT-22-70315
Revision 0

Light Water Reactor Sustainability Program

Evaluation of Physical Security Risk for Potential Implementation of FLEX using Dynamic Simulation Methods

December 2022

U.S. Department of Energy

Office of Nuclear Energy

INL/RPT-22-70315
Revision 0

Evaluation of Physical Security Risk for Potential Implementation of FLEX using Dynamic Simulation Methods

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

December 2022

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

SUMMARY

The requirements for United States nuclear power plants to maintain a large onsite physical security force contribute to their large operational costs. The cost of maintaining the current physical security posture is approximately 10% of the overall operation and maintenance budget for commercial nuclear power plants. The goal of the Light Water Reactor Sustainability Program Physical Security Pathway is to develop tools, methods, and technologies and provide the technical basis for an optimized physical security posture. This pathway will analyze and minimize the conservatisms built into current security postures in order to reduce security costs while still ensuring adequate security and operational safety. The research performed at Idaho National Laboratory within this pathway has successfully developed a dynamic force-on-force (FOF) modeling framework using various computer simulation tools and integrated them with the dynamic assessment Event Modeling Risk Assessment using Linked Diagrams (EMRALD) tool.

This document provides an overview of lessons learned in applying a dynamic computational framework that links results from a commercially available FOF simulation tool, a commercially available thermal-hydraulic tool, and EMRALD to an operating commercial nuclear power plant. This process of including plant procedures and multiple analysis results is being called Modeling and Analysis for Safety Security using Dynamic EMRALD Framework. Previous reports described how a user could integrate their plant-specific FOF models with the dynamic simulation tool EMRALD, model operator actions, integrate with probabilistic risk assessment tools, such as Computer Aided Fault Tree Analysis System or Systems Analysis Programs for Hands-on Integrated Reliability Evaluations, and with thermal-hydraulic tools, such as RELAP-5. Previous reports applied various combinations of available simulations codes with EMRALD using generic plant models to demonstrate how to perform the analysis. This report documents the results of applying the dynamic computational framework to an actual nuclear facility using their security scenarios and timelines. The purpose of this study was to verify that results achieved using generic models are similar to actual plant results and to refine our guidance of the use of the framework. Such an assessment enables further analysis, such as what-if scenarios and staff-reduction evaluation, thereby optimizing physical security at plants.

NOTE: The work performed in this report is based on a generic EMRALD model with actual plant data used for the analysis. However, only the generic model and general results of the analysis are in the report. No plant's sensitive

information is discussed in this report. The discussion shows examples of insights that can be obtained from the MASS-DEF methodology.

Page intentionally left blank

CONTENTS

FIGURES

TABLES

Page intentionally left blank

ACRONYMS

CD	core damage
DG	diesel generators
EDG	emergency diesel generator
EMRALD	Event Modeling Risk Assessment using Linked Diagrams
FLEX	Diverse and Flexible Mitigation Capability
FOF	force-on-force
INL	Idaho National Laboratory
LWRS	Light Water Reactor Sustainability
MAAP	Modular Accident Analysis Program
MASS-DEF	Modeling and Analysis for Safety and Security using Dynamic EMRALD Framework
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
O&M	operation and management
PRA	probabilistic risk assessment
PWR	pressurized-water reactor

Page intentionally left blank

EVALUATION OF PHYSICAL SECURITY RISK FOR POTENTIAL IMPLEMENTATION OF FLEX USING DYNAMIC SIMULATION METHODS

1. INTRODUCTION

The overall operation and maintenance (O&M) costs to operate a nuclear power plant (NPP) in the United States (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 (LWRS) Program 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, we 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 an NPP will need to include a reduction in labor.

To support this mission, LWRS Program established a new pathway for physical security research. The physical security pathway aims to lower the cost of physical security through directed research into modeling and simulation, the application of advanced sensors, and the 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 are 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 [2]. FLEX equipment includes 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. This more inclusive process for physical security analysis is named Modeling and Analysis for Safety Security using Dynamic EMRALD (Event Modeling Risk Assessment using Linked Diagrams) Framework (MASS-DEF).

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 NRC regulations, 10 CFR 73.55(d)(1), state, "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" [3]. 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 [4]. 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 [5].

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. Previous reports described the modeling and simulation 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. This report describes lessons learned in applying these methods at a currently operating NPP using actual scenarios, plant models, and input from their plant staff. The lessons learned from this evaluation will inform and improve future guidance documents to ensure usability and transferability to a variety of nuclear plant types, physical layouts, simulation capabilities, and organizational structures. Sections 2 and 3 provide an overview of the overall process and describe the generic model we created to facilitate easier model creation at a plant site. Section 4 describes specific observations from the evaluation at an actual plant site. This report does not disclose detailed descriptions of targets or scenarios.

2. PLANT RESPONSE WITH FORCE-ON-FORCE OVERVIEW

Traditionally, a physical security evaluation consists of evaluating if the response force can stop an attacker's objective of reaching and performing tasks on particular targets. This FOF approach is the primary defense against an attack; however, there are other facility factors to consider in an attack. This section gives a brief overview of the aspects, including plant responses, that should be considered when evaluating attack scenarios and shows the need for time-dependent modeling of these areas and potential gains or improvements from that analysis.

2.1 Force-on-Force Evaluation

The comprehensive physical security plan of a nuclear facility is evaluated both by the facility itself, and by NRC and tested through exercises. There are several FOF computational tools, such as RhinoCorp's Simajin [6] and ARES's AVERT [7] software tools, to simulate defensive strategies. This simulation allows one to review and compare defensive strategies and obtain a statistical evaluation with distributions and uncertainty bands. Researchers are using these tools to optimize security response plans, to provide good data for defense strategies and to quantify the likelihood of adversaries reaching defined objectives. A more accurate model that includes these aspects could provide grounds for further protective measure optimization, significantly reducing facility expenses.

2.2 Diverse and Flexible Mitigation Capability and Mitigation Tasks

Both during and after an attack, there are tasks that a facility may perform to mitigate actions an adversary may take or to minimize the impact of what an adversary may have achieved. For example, if an attack is detected, a control room operator may perform a task and an operator could be deployed to a strategic and protected location, or after an attack, a FLEX team could be deployed to retrieve and connect a pump to mitigate the impact of a target that was destroyed. Many tasks like these are not currently considered in physical security modeling due to the difficulty in evaluating and verifying the effectiveness given the large variance in input conditions, including timing requirements.

2.3 Timing and Plant Physics

The standard used for determining defense success or failure against an attack is typically if the attack objectives are reached. This is a conservative assumption, as there are many factors that could be considered. For example, was the reactor shut down and at what time compared to when other targets, such as cooling pumps, are destroyed. This can make a big difference in when or if CD occurs. A plant thermal hydraulics model, such as Modular Accident Analysis Program (MAAP), could be used to determine the timing and outcome of the attack scenario.

2.4 Reasonable Assurance of Protection Time

Recently, the NRC outlined the Reasonable Assurance of Protection Time (RAPT) concept [8], where, if a facility can independently protect against the design basis threat for a minimum of 8 hours, offsite help can mitigate negative outcomes. This emphasizes value for facilities to accurately evaluate time and mitigation options.

3. MODELING DIVERSE AND FLEXIBLE MITIGATION CAPABILITY AND MITIGATION TASKS

Additional tools are needed to model FLEX and other plant safety tasks as FOF simulation tools are not typically designed to handle complex procedures and dynamic options. This modeling must also include the ability to modify, run, and evaluate results from the facilities thermal hydraulics model.

Idaho National Laboratory (INL) developed EMRALD [9], a dynamic probabilistic risk assessment (PRA) tool, for other external hazard evaluations. This tool is ideal for the modeling and coupling for the MASS-DEF physical security evaluation. The INL team developed a generic EMRALD model that imports FOF data, captures general behavior for FLEX use, and can be a template for specific plant procedures or attack scenarios.

This section outlines the generic pressurized-water reactor (PWR) model that was developed in EMRALD, how it is connected to FOF simulation, the operator mitigation tasks, the thermal dynamics model, and the evaluation within RAPT criteria.

3.1 Generic Event Modeling Risk Assessment Using Linked Diagrams Model Overview

The generic model was designed to use FOF data from an FOF simulation tool, such as Simajin or AVERT. Initial coupling was done with the Simajin FOF software results to accommodate the needs of the partnering members of industry for this study. We will extend the model to include other FOF software tools and possibly statistical data. This generic model captures the well-known behavior of PWR nuclear power plants to determine if FLEX equipment could be used to prevent CD. With the generic nature of the model, the results would not be considered Safeguards Information (SGI). Once facilities add specific scenario information, procedures, or couple with site-specific FOF tools, the EMRALD model would be considered SGI and would need to be protected according to 10 CFR 73.20 and 73.21.

The generic model incorporates basic PWR safety elements, such as the control room, diesel generators (DG's), motor-driven pumps, turbine driven pumps, condensate storage tanks, water tanks, etc., as shown in Figure 1. Each component is modeled separately with probabilistic transitions between startup, operational, and failed states, along with failure links that come from the FOF simulation data and as informed by the PRA model. All of these components can be set to fail according to the time specified by the FOF results, or if a specific plant does not have the component, such as a second motor-driven pump, it can easily be removed.

Figure 2 shows an example component model for the DG. The StartingDG1 event is a distribution on the time it takes to start up the generator. When the startup demand comes, the generator may start successfully or fail to start. If it starts, the simulation goes to the DG1Running state and transitions to the DG1Failed state if it has random failure or if there is a time set that it is hit by an adversary.

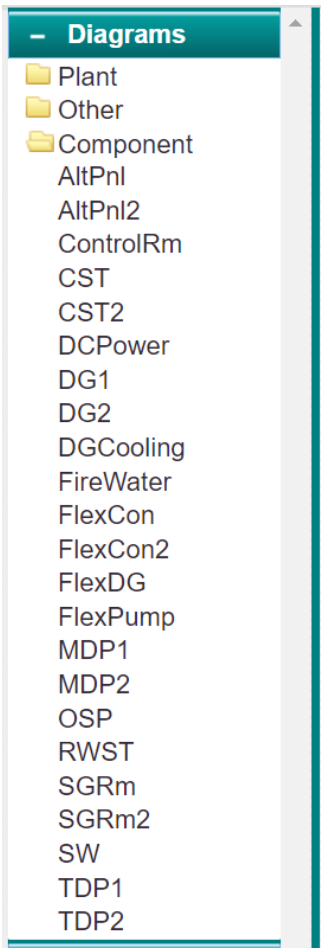

Figure 1. Reactor components in EMRALD.

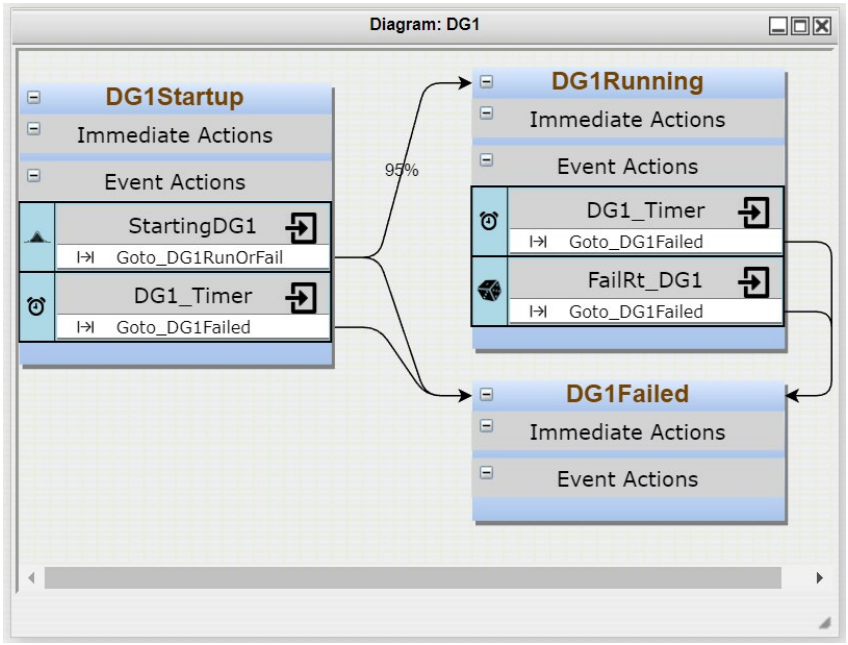

Figure 2. DG operational diagram.

DGs start when the offsite power is lost. However, there is a possibility that the adversaries target the generators after they start to operate. The operational status of the generators needs to be monitored. The FOF simulation (Simajin) provides the time data when the generators are sabotaged. This data is recorded in EMRALD variable EDG1_HitTime and EDG2_HitTime for the first and second generator, respectively. The DG1_Timer event shown in Figure 3 uses this timing variable to switch the generator state from DG1Running to DG1Failed. With this modeling approach, the generators may run for some time before they are sabotaged. These dynamics can be fed into a reactor safety analysis code to evaluate the resulting reactor state.

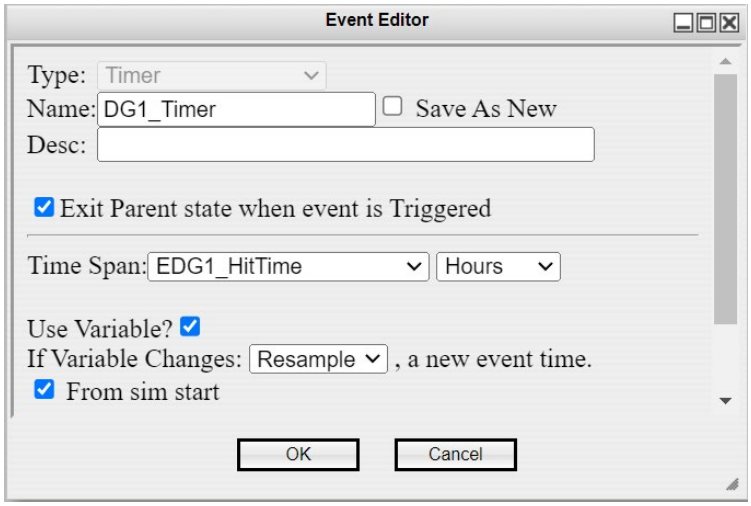

Figure 3. DG1_Timer event in DG1Running state.

Figure 4 shows a simple type of component model that only uses two states. The initial state (SGRmRunning) is active from the start of simulation; therefore, it is not necessary to call it exclusively by using a transition action. The component may transition to the failed state if it is sabotaged by adversaries (modeled by the SGRm_Timer) or if any random failure happens stochastically (modeled by the failure rate event FailRt_SGRm).

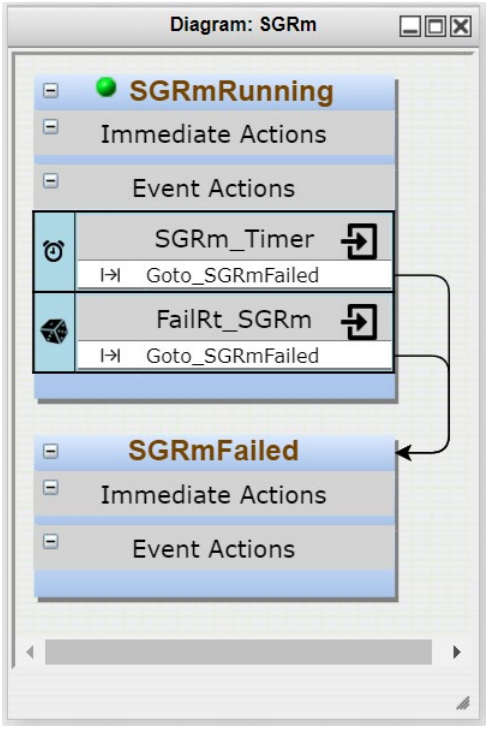

Figure 4. Switchgear room diagram.

3.2 Integrating FOF Data in a Generic Model

The generic model has an "Initiate_Attack" diagram that runs the FOF attack results and starts the other aspects of the model, as shown in Figure 5. The AttackSetup state begins at the start of simulation and immediately executes the Goto_Process_FoF_Runs transition action. This action activates the Process_Simanij_Run state that extracts output variables from the Simajin FOF software, assuming that it is simulated in advance. Otherwise, the state may be modified to execute the Simajin simulation and read its output afterwards. After reading Simajin's output file, the AttackDetected event is activated after a certain delay time, governed by the output data from Simajin. The event triggers the FoF_Engagement state, which waits for the specified amount of time for the attack to complete, again by using the time data from Simajin. After the attack ends, a team of armed responder is dispatched to sweep the plant and ensure it is secure for safety personnel to initiate FLEX mitigation actions if needed. This procedure may differ for each plant. For example, a plant with pre-deployed FLEX equipment in a secured room may choose to dispatch FLEX operators early upon detection of an attack.

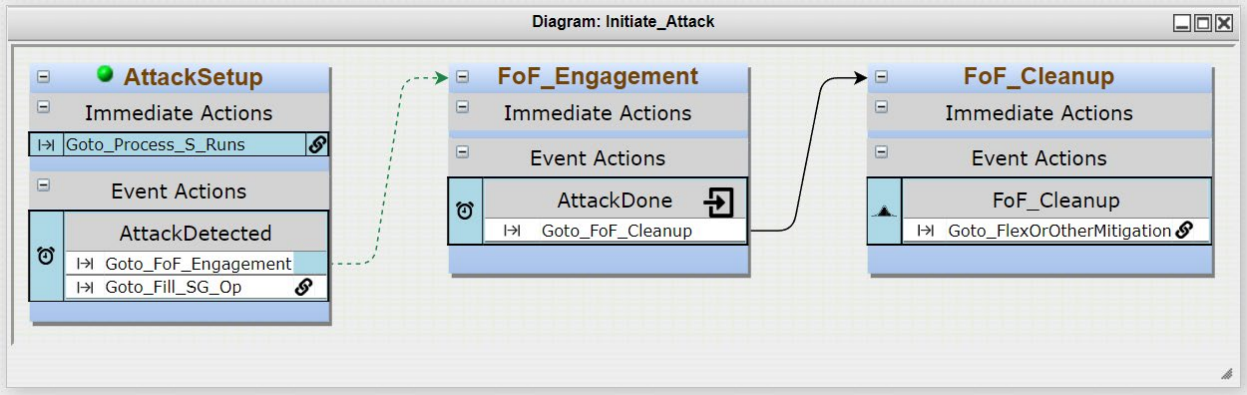

Figure 5. EMRALD attack scenario.

The Process_Simanij_Run state shown in Figure 6 reads the sabotage timing data for each possible target in a generic PWR plant. Users may add or remove this data according to their plant-specific target sets.

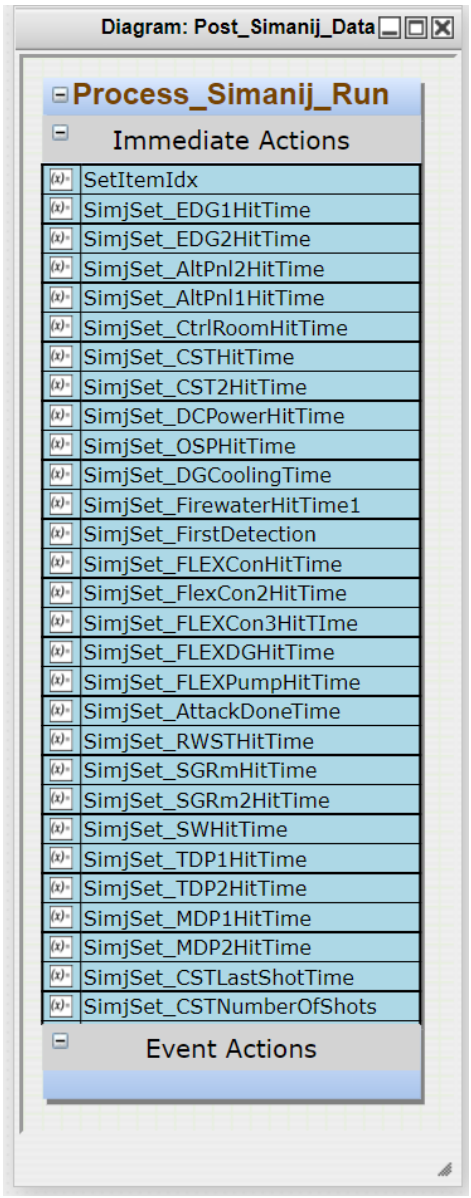

Figure 6. Process_Simanij_Run state.

The actions in the Process_Simanij_Run state rely on variables coupled with the extensible markup language (XML) output file of Simajin software. Figure 7 shows a sample of this variable for emergency diesel generator's (EDG) sabotage time. The Doc Path field locates the path to Simajin's XML output file, while the Var Link field describes the XPath expression needed to extract a particular data from the XML file, which, in the case of Figure 7, is the value of EDG1_breach_time data. If EDG1_breach_time data is not found in the XML file, EMRALD returns a default value of 0, which implies that EDG1 is never sabotaged in the attack scenario. To use data from another FOF simulation tool, similar variables can be linked to result data from that tool for each item that belongs to a scenario target set.

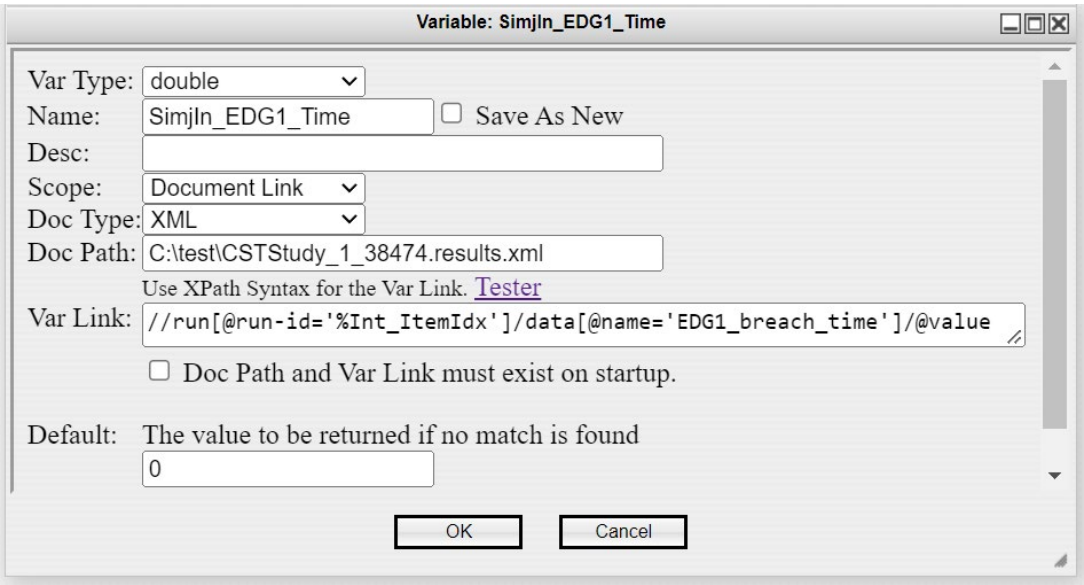

Figure 7. XML-linked variable of the EDG sabotage time.

3.3 Operator Procedures Generic Model

There are two types of operator procedures that can be part of the model. The first set includes actions that could be taken upon detecting an attack. The second set includes actions that could be taken after the attack and physical security has cleared the site and can support operator movements.

3.3.1 On Attack Response Procedures

The generic model allows for multiple procedures to be added once an attack is detected. This is done by creating a new diagram in EMRALD, modeling that procedure, and then adding a link to start that procedure in the "AttackDetected" event under the "AttackSetup" state in the "Initiate_Attack" diagram, as shown on the left side of Figure 8. For this pilot, the pilot facility wanted to explore the option of filling the steam generators, as long as filling equipment was available, up to 80%. The filling procedure would begin as soon as an attack is detected.

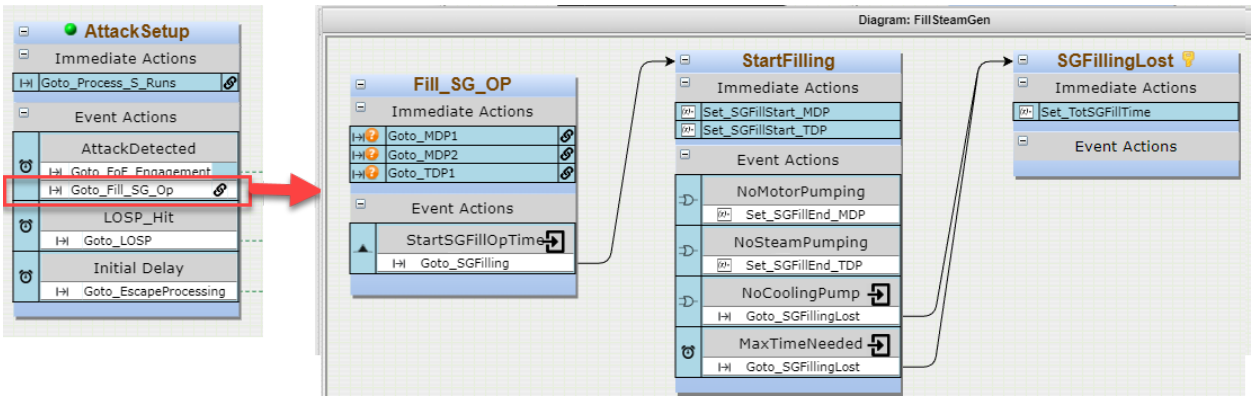

Figure 8. (Left) Attack detection triggering evaluation of the EMRALD diagram (Right) of the procedure to fill the steam generator on detection of an attack.

Filling the steam generators provides a larger inventory of cooling water if an attack is successful at disabling other forms of heat removal. There are three states in the fill procedure: Fill_SG_OP, StartFilling and SGFillingLost. In the first state "Fill_SG_OP", the fill pumps are verified available, then

the time it takes the operator to verify the attack alarm and start the filling process is represented by the distribution event “StartSGFillOpTime”. An initial normal time distribution value of 30 seconds with a standard deviation of 5 seconds was used for the "StartSGFillOpTime” event. Research would need to be done to determine accurate times for this procedure before actual credit of this procedure can be taken. Once this time is up, the simulation moves to the “StartFilling” state in the diagram. Here, the system waits until either all the filling pumps have failed or the maximum time needed to fill the steam generator has expired, before moving to the third state in the diagram, i.e. the “SGFillingLost” state.

3.3.2 After Attack Mitigation Procedures

The “Attack_Response” diagram is executed after the sabotage attack and is shown in Figure 9. Using FLEX was implemented for this pilot project. First, the model evaluates if FLEX is needed then starts the simulation piece for the FLEX procedures. An example mitigation action is provided when a loss-of-offsite-power event happens. It activates the DGs and their cooling system. If backup power from generators is not available, the plant enters the “station blackout” state, and the “Need_DC_Power” event is triggered. If the design basis safety system can mitigate the sabotage, the “FlexNotNeeded” event is active and brings the plant to the “Safe_Shutdown” state. Otherwise, the FLEX equipment needed is determined by a logic tree evaluation, either FLEX generator or pump. The logic trees evaluate equipment failures, triggered from the FOF data. For example, the “NoBackupPower” logic tree in Figure 10 evaluates if the DGs, switchgear, and cooling to determine backup power availability. General trees are provided in the generic model and can be adapted for specific plants. For the pilot scenario, we determined that only the FLEX pump was needed for their scenarios.

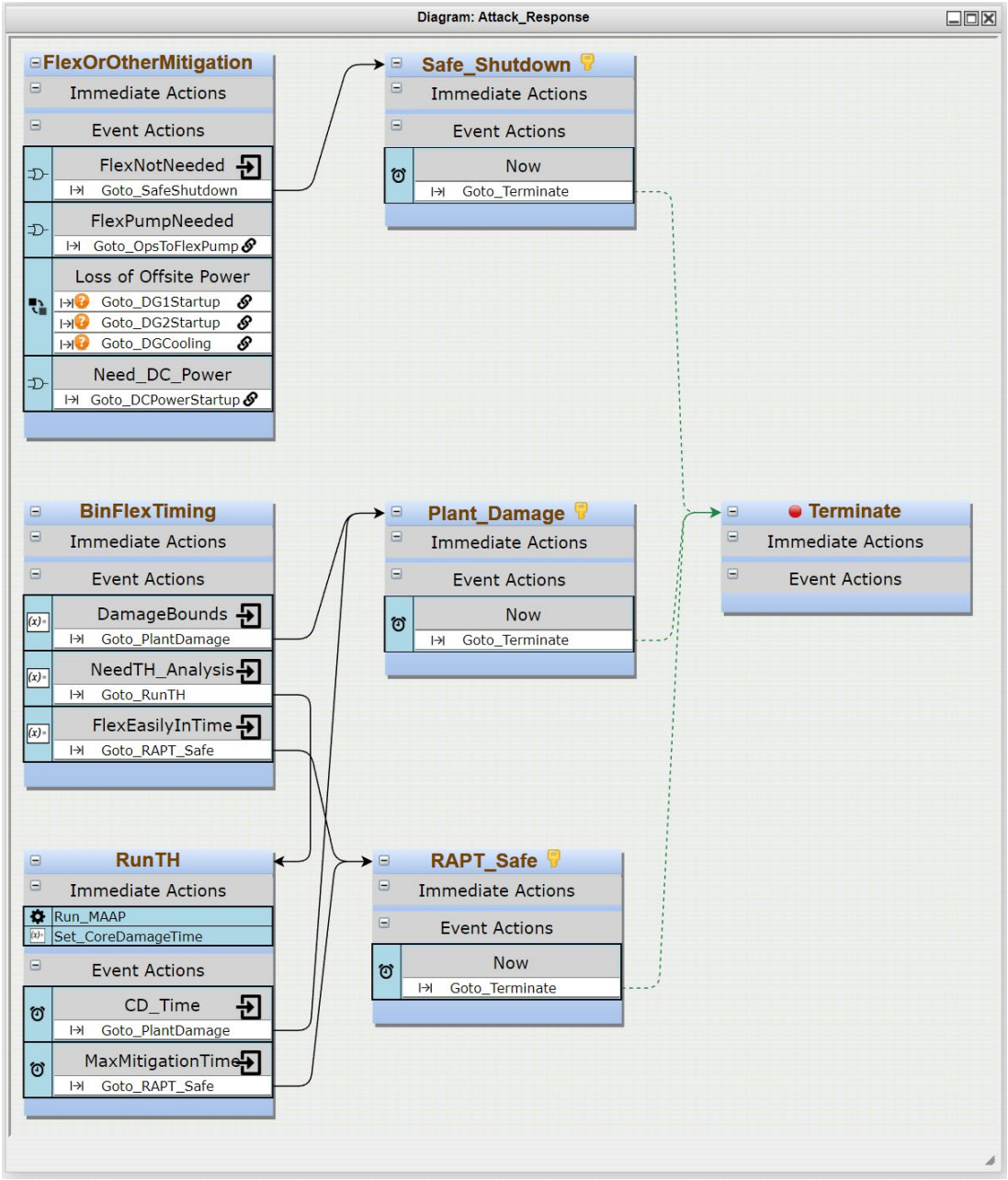

Figure 9. The Attack_Response diagram evaluates and starts FLEX, evaluates procedure times, and runs thermal hydraulics to determine plant damage.

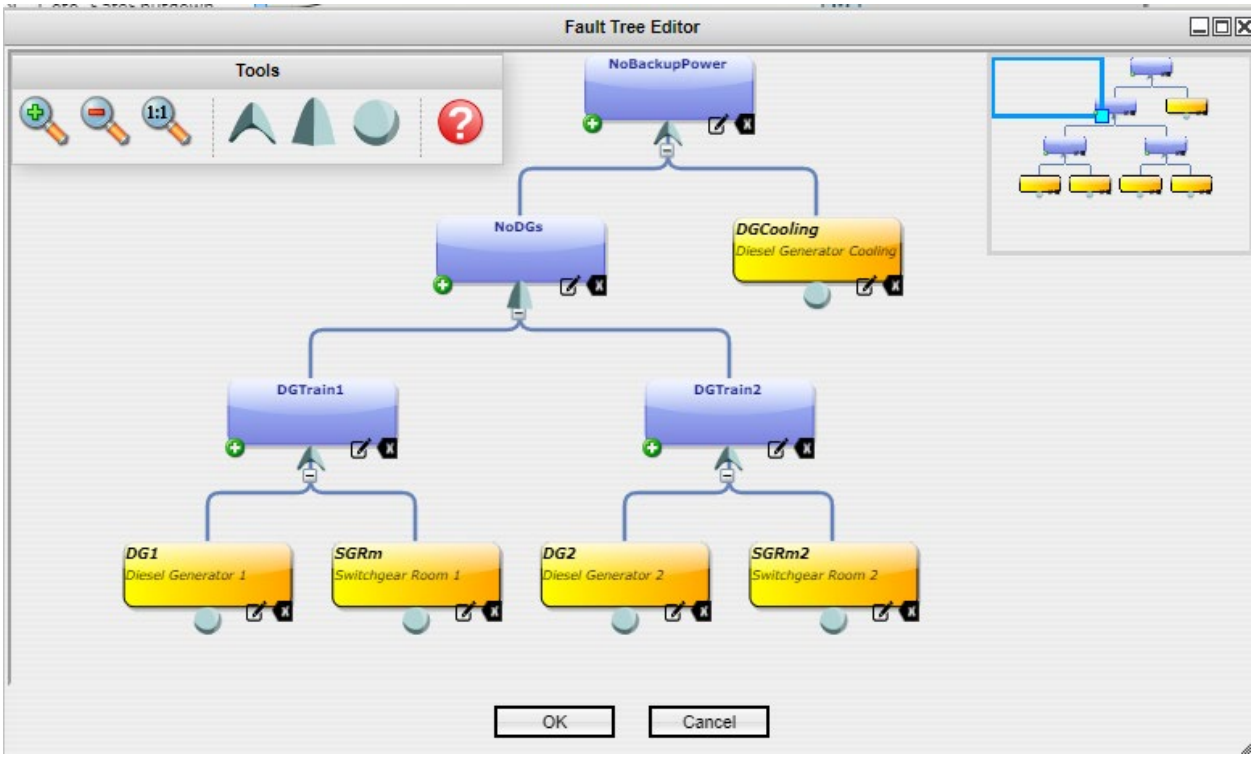

Figure 10. The logic tree for NoBackupPower event evaluates if backup power is needed depending on component availability.

The FlexPumpNeeded event shown in Figure 9 is triggered when the installed feedwater system is unavailable, either due to malfunctions or a sabotage, and operators execute the FLEX pump strategy shown in Figure 11. The steps in this diagram are generic and can be easily applied to any plant. Users may tailor this diagram further according to their plant-specific FLEX procedures. The diagram starts from OpsToFlexPump state where operators are dispatched to go to the FLEX storage building. The OpsTimeToFlexBuilding event contains the statistical distribution of operators' travel time to the building, while the MaxMitigationTime event is the maximum time window beyond which the FLEX strategy cannot be deployed. ClearFLEXRoute state models the step when operator uses the equipment in the storage building to clear the route from debris (if any) for FLEX pumps. The TransportFLEXPumps state contains the operator action to mobilize the FLEX pump from the storage building to its staging area. The DepressurizeSG state contains the action to depressurize the secondary line to allow the FLEX pump to inject water. At this point, the operator may discover that the FLEX pump connection points are sabotaged by adversaries and that, therefore, the FLEX pump strategy cannot be used, and the simulation goes into the "No FLEX" state. The "FLEX Pump to Suction" state models the action to connect the FLEX pump to the suction points, at which point the operator may discover that adversaries have sabotaged the water sources / storage tanks. In such a case, the simulation goes to the "No FLEX" state. Otherwise, the operator continues to connect the FLEX pump discharge port and align the valves to have the FLEX pump ready for operation. When the FlexPumpReady state is active, it executes the FlexPump component diagram in Figure 12. The pump has a 3.38E-2 fail-to-start probability and a 1.55E-2 running failure rate with a mission time of 24 hours. These failure rates are taken from PWR Owner's Group's open publication in February 2022 (PWROG-18042-NP Rev 1). If the pump fails within its mission time, another backup pump is retrieved from the FLEX storage building through the NeedAnotherFlexPump event. If the FLEX pump runs successfully, the simulation executes the Goto_EvaluateTiming action to run the BinFlexTiming state in Figure 9.

Each of the procedure steps have a distribution time associated with it for how long the operators take. The generic model has arbitrary numbers assigned, but for the pilot project, testing times and expert judgement were used to assign the distribution parameters. The steps are fairly generic, so that small steps could be grouped into the steps modeled; however, additional steps could be added for a specific facilities' need.

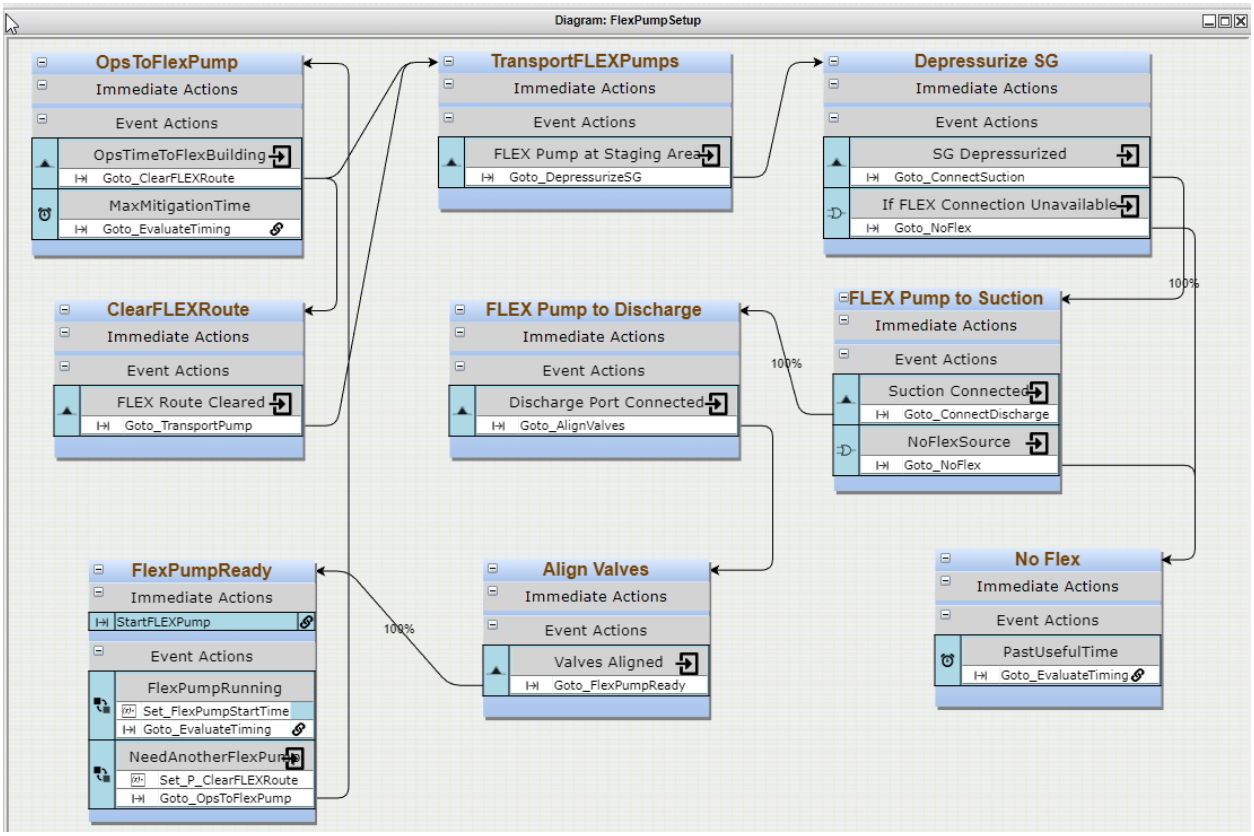

Figure 11. FlexPumpSetup diagram modeling the procedures with timing and failure options in setting up a FLEX pump.

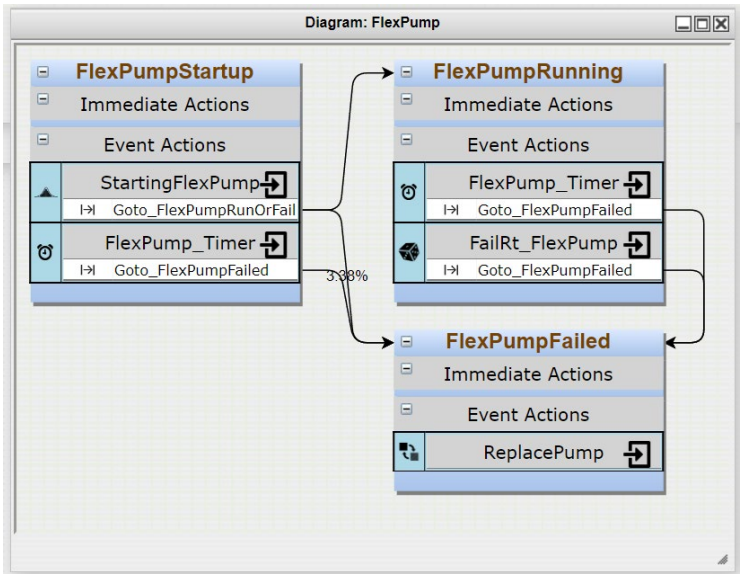

Figure 12. FlexPump diagram modeling the behavior of a FLEX pump, including its operational states and how it can fail.

3.4 MAAP Model

In order to effectively determine if or when CD occurs, researchers need a thermal hydraulics model. This model needs to have parameters to set times for the loss of the various cooling options and include features for FLEX cooling along with a set time parameter. For the pilot, the plant provided a MAAP model. As they wanted to evaluate filling the steam generator during an attack, they also modified this model to include a start and end time for the filling activity. The MAAP input file provided used input blocks to evaluate the current time against a specified time to trigger the filling, cooling, and FLEX pump conditions, as shown in Figure 13. This input file can be modified by EMRALD to set the times according to the times they occur in the simulation.

```
WHEN TIM >= 0.0 S
IEVNT(224) = F // MOTOR-DRIVEN Aux Feed in auto
END
```

Figure 13. Example of MAAP input block to set the motor-driven pump to fill the steam generator starting at time 0.

3.5 EMRALD-MAAP Integration

Once the FLEX procedures are executed, the simulation enters the RunTH state if preset criteria cannot easily determine safe shut down or CD, and the MAAP thermal hydraulics tool is used to determine CD using EMRALD's external application option. EMRALD has a custom form in development for MAAP, which allows the user to easily link EMRALD variables to fields in MAAP, as shown in Figure 14. After loading an existing MAAP file, the parameters, initiators, and input blocks can be seen and assigned to use variables inside EMRALD, as outlined in red in Figure 14.

For the pilot project, a few MAAP parameters are dynamically set. First, the start time for filling the steam generators using either the motor or steam driven pumps is set. Then, the end time for cooling systems and filling the steam generators is set. Finally, the FLEX or firewater injection start time is assigned. After MAAP has been executed, one of the standard outputs is the core uncover time. EMRALD can directly read this value, so it is used as a conservative value to indicate possible CD.

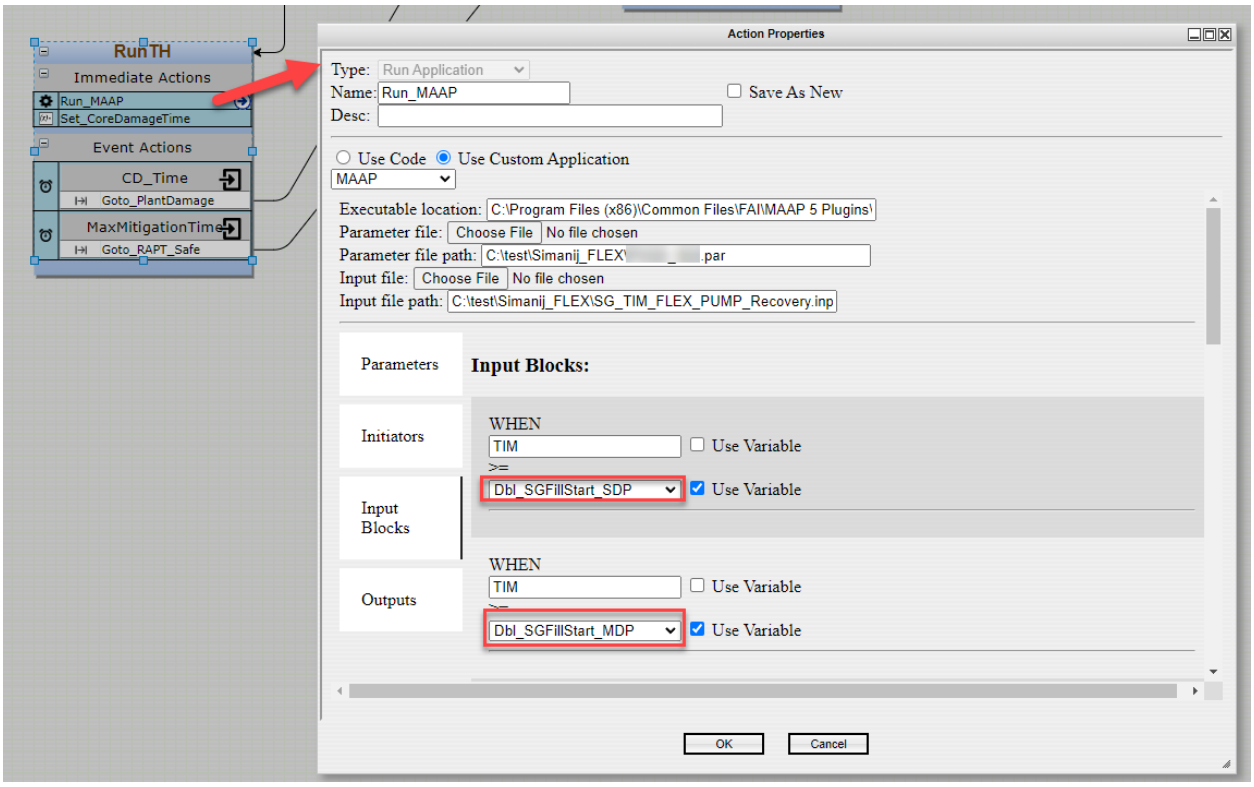

Figure 14. EMRALD form to set up MAAP execution and get results.

3.6 EMRALD Integrated Results

The model described above can be used to evaluate specific attack scenarios or all the scenarios combined. For each of the FOF simulation runs, EMRALD processes the attack outcomes and performs an EMRALD evaluation run. Each run will end in either the Safe_Shutdown, Plant_Damage, or RAPT_Safe key state. Safe_Shutdown indicates that defensive measures and standard plant safety systems prevented CD. Plant_Damage indicates that adversaries achieved their objectives, the standard plant safety systems were not available, and FLEX or other after attack mitigation options failed or could not be engaged in time. RAPT_Safe indicates that standard plant safety equipment was not available, but that FLEX or other after attack mitigation options prevented CD until at least the specified time needed for the RAPT criteria. EMRALD results divide the count of different key states by the total number of runs to give a probability for the outcomes and calculates a standard deviation.

The EMRALD analysis results should be verified using several methods before implementation or submission to the regulator. Tabletop exercises would be the first step in verifying the modified protective strategy. The use of limited scope performance tests and FOF exercises to validate the EMRALD results with real-world test data would also provide a test of the EMRALD analysis accuracy and justification for protective strategy changes to the regulator. Using EMRALD allows researchers to include safety actions and dynamic scenarios in addition to the capabilities found in FOF software. It allows licensees to provide technical justification to optimize their physical security posture in compliance to RAPT.

4. ACTUAL SAMPLE PLANT EVALUATION

A collaborating utility is working with INL and RhinoCorps to evaluate if including FLEX and other operator procedures in a security plan can reduce personnel resources needed to protect required

equipment and prevent plant CD for their attack scenarios. While this is an ongoing activity, this section outlines the steps and outcomes learned by applying previously developed methods to an actual plant. For more information on the FOF & EMRALD modeling and the process to optimize defense strategy see Reference [10] and [11].

4.1 Scenario Review

The first step in performing this type of security risk evaluation is to review the existing attack scenarios and determine which scenarios include damage to equipment that could reasonably be mitigated using FLEX equipment or other operator actions. To do this, researchers should conduct a review with operations, PRA, and security experts. Since the evaluation will require access to SGI, care must be taken to ensure selected staff have SGI access. During this review, the team should evaluate FLEX and other accident mitigation procedures to identify equipment that could reasonably prevent CD if plant equipment was damaged in an attack.

For the example evaluation, the collaborating site provided experts from security, operations, PRA, and FLEX system engineers. The team reviewed existing security scenarios by target, difficulty to protect against, and after attack mitigation options. The review determined that fire water injection into the steam generator or a FLEX pump providing cooling to the steam generator could be used to mitigate several scenarios. There were several scenarios where a FLEX generator could be beneficial, but the pump would also work as a mitigation. The FLEX pump was also slightly faster to transfer and hook up, so only the FLEX pump was used in the analysis.

4.2 Force-on-Force Model Modifications

In order to credit FLEX or other operator procedures, attack targets that could prevent the use of these mitigating features need to be added to the FOF simulation target sets. There are multiple ways to disable FLEX, so an expert evaluation of the procedures in addition to a plant walkdown may be needed to identify vulnerable locations. The team should evaluate the FLEX pumps, FLEX storage locations, transportation routes, suction connections, discharge connections, and plant valves and pipes that are part of the injection flow path. Those portions of the flow path near existing targets should be looked at closely.

The team performed this process as part of the example utility evaluation, including a detailed plant walkdown, and identified the more vulnerable attack points for the potential FLEX implementation. These attack points were then added to the existing attack scenarios in the FOF simulation model.

4.2.1 Test Force-on-Force Runs

Before connecting EMRALD to the FOF results, an initial analysis determined if the FLEX and other operator procedures could be effective by putting the main targets in one group and the FLEX in a separate group in order to evaluate if the adversaries were able to damage just the main targets or both the main targets and the FLEX targets.

Table 1 shows a hypothetical example of a few scenarios and their results before using the FOF data in the EMRALD model. The “Original Model” column shows the percentage of safe vs. main targets hit, before any defense-in-depth modifications are added. “Initial Defense-in-Depth with FLEX” shows the percentage of safe, main targets hit, and both main and flex targets hit. The “Main Only” field indicates the maximum benefit FLEX or other operator procedures could provide if all were successful. The ideal case for the maximum FLEX benefit would be for the “Main Only” column to be as close to 100% safe as possible with a very low “Main & FLEX” percentage, such as in Row S2. In Table 1, Scenario 1 is a significant contributor to a physical security risk and FLEX could reduce that risk by 50%. For Scenario 2, FLEX could help significantly, but in Scenario 3, the adversaries are always able to prevent FLEX use.

Table 1. Example of scenario evaluation when including FLEX procedures.

Scenario	Original Model		Initial Defense-in-Depth with FLEX			Modified Defense-in-Depth with FLEX		
	Safe	Main	Safe	Main Only	Main & FLEX	Safe	Main Only	Main & FLEX
S1	85%	15%	50%	25%	25%	50%	35%	15%
S2	90%	10%	70%	25%	5%	70%	30%	0%
S3	95%	5%	80%	0%	20%	50%	5%	15%

4.2.2 Modifications to Improve FLEX

The next step in the process is to evaluate the results of the initial FOF simulations to determine how the FLEX option might be eliminated during the attack scenarios. Security experts should be the ones evaluating the results and may be able to identify modifications to the defensive strategy that could significantly improve the outcome. Proposed updates to the defensive strategy need to be made to the FOF model to generate new results. It may take several iterations to identify the most efficient strategy to protect both the existing plant and FLEX equipment.

For the example evaluation, we discovered that adding FLEX could only improve a couple of the scenarios and did not provide a significant improvement for a critical scenario. Upon review, this was because the existing defensive strategy was not designed to protect FLEX connections and allowed FLEX pump connections to be easily accessed by adversaries. To improve the result, we made a few modifications, including modifying the roaming and protection area for some guards and patrol vehicles and adding a delay barrier to the FLEX pump connection location. After these modifications to improve FLEX protection, the data for the third column, “Modified Defense-in-Depth with FLEX” of Table 1, can be added. In this hypothetical example, S1 is improved significantly, which would make the biggest difference for the overall results.

4.3 Guard Reduction

The increased margin achieved by implementing FLEX and other operator procedures in the security plan could allow for the removal and shifting of existing guard posts. Some scenarios require additional guards to protect against specific targets, by adding the FLEX targets for those scenarios, existing guards can now protect against those scenarios, given that FLEX options can recover from primary target sabotage. The iterative method shown in Figure 15 and outlined in Reference [11] is being used to optimize posts while maintaining the security effectiveness at an equivalent level.

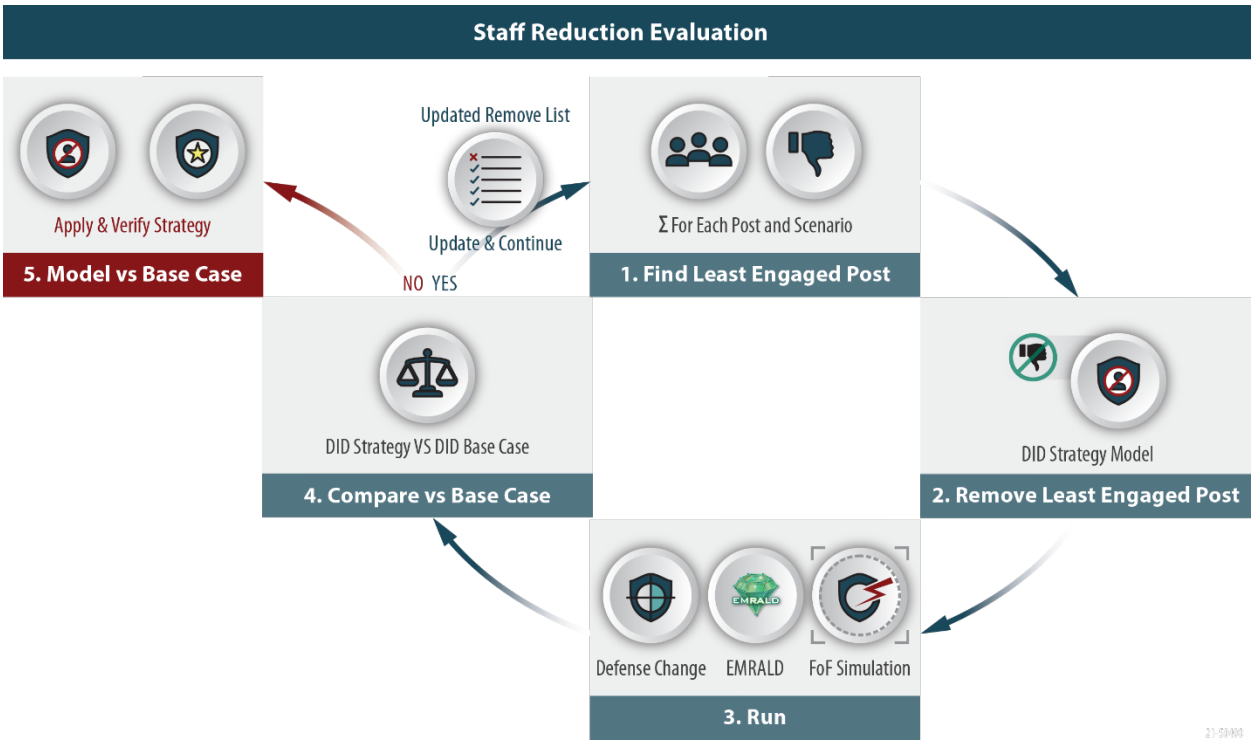

Figure 15. Guard post reduction method process to maintain protection equivalency.

5. RESULTS, OBSERVATIONS, AND FEEDBACK

Initial feedback from industry security professionals indicated that they do not want complex models that they have to maintain in order to include operator procedures and FLEX in physical security. This feedback prompted the development of a generic model that can be used by multiple facilities as a starting template model of their plant-specific procedures. Using a generic model will significantly streamline the process of performing a similar analysis by another utility.

The generic PWR EMRALD model has been successful in this example security risk assessment evaluation. It successfully pulls in data from Simajin, simulates plant FLEX procedures, and runs the MAAP thermal-hydraulic code to determine scenario outcomes.

Initial results showed that the time window, i.e. remaining time between the end of the engagement and including a sweep of the facility to ensure no further adversaries pose a threat and the general time to inject cooling before CD, may be less than the time needed to deploy FLEX depending on where the FLEX equipment is stored. However, this limited time window may be extended by sufficiently filling the steam generators when an attack occurs. Depending on the available fill time, the steam generators could possibly provide adequate time for a FLEX procedure implementation. A general observation from adding FLEX to physical security is that, to be effective, several factors may need to be addressed:

- Ensure there is enough time to deploy FLEX strategy, through either of the following:
  - Pre-stage FLEX equipment somewhere easily protected through physical security measures
  - Add procedures to fill steam generators to a higher level when an attack is detected
- Ensure a sufficient physical protection of FLEX equipment

- Connections or pre-staged equipment should be strategically located for easy protection away from target set equipment locations
- Connections or pre-staged equipment should have an access delay.

Another observation was that fire water injection could be a more feasible alternative than using FLEX equipment. This option needs further evaluation to determine if it will be feasible to implement, will provide the required core cooling, and could be adequately protected. Other options to consider could be firetrucks or other water sources available for injection. In some cases, existing plant connections may be vulnerable to attack, but other options may be available with a simple modification that could be easier to defend against attack.

6. CONCLUSION AND FUTURE WORK

This report builds on previous work completed within the LWRS Physical Security Pathway. Previous studies developed a dynamic computational framework that links results from commercially available FOF simulation tools, commercially available thermohydraulic tools, and the dynamic risk modeling tool EMRALD to more accurately model the complex nature of physical security scenarios and the time-dependent nature of how CD could occur during these scenarios. This more inclusive process for physical security analysis is named MASS-DEF. Previous studies developed and demonstrated the functional connection between the required applications using generic PWR physical security and reactor models. Initial results using the generic models looked promising, and the research has proceeded to the next step. In this report, we applied the MASS-DEF process to an actual commercial NPP to verify that results obtained using generic models were representative of actual scenarios and to further refine the guidance to support future analysis by other utilities. As part of this research, we developed a generic EMRALD model to reduce the modeling effort that a utility would need to perform to replicate this type of analysis. In this analysis, we obtained reasonable results and identified several valuable insights about the potential effectiveness of crediting FLEX equipment in security scenarios. We collected feedback from the utility regarding both the process and result analyses. The lessons learned from this study will be used to work with industry to create a guidance document outlining a detailed process to perform this type of analysis.

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. Nuclear Energy Institute. 2016. “Diverse and Flexible Coping Strategies (FLEX) Implementation Guide.” NEI 12-06, Rev. 4, Nuclear Energy Institute
3. 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.
4. 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.

5. 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.
6. RhinoCorps Ltd. Co. 2021. “Rhino Corps Homepage.” Accessed July 28, 2021. https://www.rhinocorps.com.
7. ARES Security. 2022. “AVERT Suite.” Accessed November 14, 2022. https://aressecuritycorp.com/software/avert-suite.
8. U.S. Federal Register. 2020. “Physical Protection Programs at Nuclear Power Reactors Safeguards Information”. Accessed November 17, 2022. https://www.federalregister.gov/documents/2020/11/30/2020-26273/physical-protection-programs-at-nuclear-power-reactors-safeguards-information
9. Idaho National Laboratory. n.d. “EMRALD.” Accessed July 28, 2021. https://emrald.inl.gov/SitePages/Overview.aspx.
10. R. Christian, S.R. Prescott, C. P. Chwasz, V. Yadav, and S. W. St. Germain. 2021. “Guidance Document for Using Dynamic Force-on-Force Tools.” INL/EXT-21-64214, Rev. 0, Idaho National Laboratory.
11. R. Christian, V. Yadav, S. R. Prescott, and S. W. St. Germain. 2022. “A Dynamic Risk Framework for the Physical Security of Nuclear Power Plants.” Nuclear Science and Engineering. https://doi.org/10.1080/00295639.2022.2112899.