INL/RPT-23-73490
Revision 1

Light Water Reactor Sustainability Program

Plant-Specific Model and Data Analysis using Dynamic Security Modeling and Simulation

November 2023

U.S. Department of Energy

Office of Nuclear Energy

INL/RPT-23-73490
Revision 1

Plant-Specific Model and Data Analysis using Dynamic Security Modeling and Simulation

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

November 2023

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

SUMMARY

The requirements for U.S. nuclear power plants to maintain a large on-site physical security force contribute to their high 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 (LWRS) program's physical security pathway is to develop tools, methods, and technologies and provide the technical basis for an optimized physical security posture. The conservatisms built into current security postures may be analyzed and minimized in order to reduce security costs while still ensuring adequate security and operational safety. The research performed at Idaho National Laboratory within LWRS program's physical security pathway has successfully developed a dynamic force-on-force modeling framework using various computer simulation tools and integrating them with the dynamic assessment Event Modeling Risk Assessment using Linked Diagrams (EMRALD) tool.

This document provides an update on the progress in applying a dynamic computational framework that links results from a commercially available force-on-force simulation tool, a commercially available thermal-hydraulic tool, and EMRALD to an operating commercial nuclear power plant. This report is only a summary of the progress and does not contain specific modeling results as those contain sensitive security information. This process of including plant procedures and multiple analysis results is being called Modeling and Analysis for Safety Security using Dynamic EMRALD Framework or MASS-DEF. Previous reports described how a user could integrate their plant-specific force-on-force models with the dynamic simulation tool EMRALD, model operator actions, integrate with probabilistic risk assessment tools, such as CAFTA (Computer Aided Fault Tree Analysis System) or SAPHIRE (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. **This report does not contain any plant's sensitive information and/or Safeguards Information.** 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 on the use of the framework. This assessment enables further analysis, such as what-if scenarios and staff-reduction evaluation, thereby optimizing physical security at plants.

Page intentionally left blank

CONTENTS

SUMMARY iii

ACRONYMS vii

1. INTRODUCTION 1

2. METHODOLOGY 2
   2.1 Physical Security Analysis Tool: Simajin 4
   2.2 Safety Analysis Tool: MAAP 5
   2.3 Dynamic Simulation Tool EMRALD 5

3. PLANT-SPECIFIC MODEL 5
   3.1 General Information of the Plant 6
   3.2 Physical Security Analysis Model 6
   3.3 MAAP Model 7
   3.4 EMRALD Model 7
      3.4.1 Model Development 7
      3.4.2 Model Simulation 7

4. RESULTS AND DISCUSSIONS 8
      4.1.1 Initial Preventive Strategies 8
      4.1.2 Improved Preventive Strategies 9
      4.1.3 Guard Post Reduction 10

5. SUMMARY AND FUTURE WORK 11
   5.1 Hypothetical Next Steps for the NPP 14

REFERENCES 15

FIGURES

Figure 1. Methodology flowchart 3

Figure 2. Example of MAAP input block to set the motor-driven pump to fill the steam generator starting at time 0. 7

Figure 3. Left: EMRALD variable for electric diesel generator attacked time. Right: Simajin results for the sabotage time. Variable names between the two models must match. 8

Figure 4. Data and interactions between the tools used. 8

Figure 5. Reduction of adversary success rate when including the FLEX pump. 9

Figure 6. The different NRC regulations a licensee could consider for their updated physical security plan. 12

Figure 7. Flowchart for PSP effectiveness evaluation for regulatory considerations. 13

TABLES

Table 1. Comparison showing a few of the exaggerated scenario's results with added targets and EMRALD simulation results. 10
Table 2. Comparison showing a few of the exaggerated scenario's results with added targets and EMRALD simulation results. 10

Page intentionally left blank

ACRONYMS

CD	core damage
DOE	Department of Energy
EMRALD	Event Modeling Risk Assessment using Linked Diagrams
EPRI	Electric Power Research Institute
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
MODSIM	Modeling and Simulation
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
O&M	operation and management
PRA	probabilistic risk assessment
PSP	physical security plan
PWR	pressurized-water reactor
SAPHIRE	Systems Analysis Programs for Hands-on Integrated Reliability Evaluations
SGI	safeguards information

Page intentionally left blank

PLANT-SPECIFIC MODEL AND DATA ANALYSIS USING DYNAMIC SECURITY MODELING AND SIMULATION

1. INTRODUCTION

Operation and maintenance (O&M) of several nuclear power plants (NPP) in the United States have become financially burdensome, to the point that the utilities may have to stop operation and retire their plants prior to the expiration of their operating license due to economic pressure. Moreover, the wholesale electricity prices have declined in some markets due to the increased penetration of renewables, such as wind and solar power, and the continued use of natural gas power. This phenomenon reduces NPPs' income from power generation. As a result, NPP operators aim to lower their O&M cost to ensure the plants can continue to produce electricity competitively.

The Department of Energy (DOE) has established the Light Water Reactor Sustainability (LWRS) program to assist NPP operators in sustaining their plant operations. The program has identified that 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]. Within this overall labor cost, nearly 20% of it is needed to maintain the labor in physical security forces. The Nuclear Regulatory Commission (NRC) security requirements for commercial operating nuclear sites increased exponentially following the September 11th terrorist attacks resulting in a significant increase of onsite response force personnel across the nuclear industry [2]. The plant's response force includes the minimum number of armed responders, as required in 10 CFR 73, and security officers tasked with assigned duties, such as stationary observation / surveillance posts, foot-patrol, roving vehicle patrols, compensatory posts, and other duties as required [3]. Since labor costs continue to rise in the United States, any effort to reduce O&M costs needs to include a reduction in labor.

To support this mission, the LWRS program has established a 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. These efforts are expected to reduce an NPP's dependency on labor work in the physical security area. Modeling and simulation are used to evaluate the margin inherent in many security postures and 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 [4] and actions taken by operators to minimize the possibility of reactor damage during an attack scenario. 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).

Work started last year to apply the MASS-DEF methodology on an actual NPP in the United States [5] on several example attack scenarios. This work extends the previous work by including more scenarios, making proposed changes to an actual plant security model, and utilizing recent technical feedback received from the industry. The results of this study will be used to investigate the possibility of reducing the number of armed responders required on site to maintain adequate protection of the facility.

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 a typical physical security posture model 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. A future report will discuss the level of post reduction that may be achieved by this addition to the security plan and cost comparison of the labor saved vs. the cost to implement these changes.

2. METHODOLOGY

The conventional method to evaluate the effectiveness of a physical protection system is to run numerous physical security simulations up to the point when the attackers manage to reach vital areas identified as target sets. This approach removes the complexity of how the protected structures and systems work, such that the analyst can focus on designing the physical protection system. However, there are other factors that can be credited before and after the attackers manage to successfully sabotage the nuclear plant equipment, for example, estimating the time it takes for the plant to undergo a catastrophic damage, executing preventive safety actions within that timeframe to prevent such a damage, or perhaps even performing preliminary safety actions before attackers sabotage a target. These factors can be credited by incorporating them in the modeling and simulation framework together with the physical security model.

The methodology used in this work is described in Figure 1. The first step is to identify the specific nuclear plant and its associated attack scenarios or target sets that could be prevented using possible safety actions. An initial testing to evaluate the effectiveness of preventive actions is done by simulating those attack scenarios while including the safety equipment in the target sets. This test should provide insights on whether the safety actions could prevent damage to the reactor core effectively, or whether improvements are needed to protect the safety equipment, to reduce the action times, etc. The computer models should be updated with these improvements, if any.

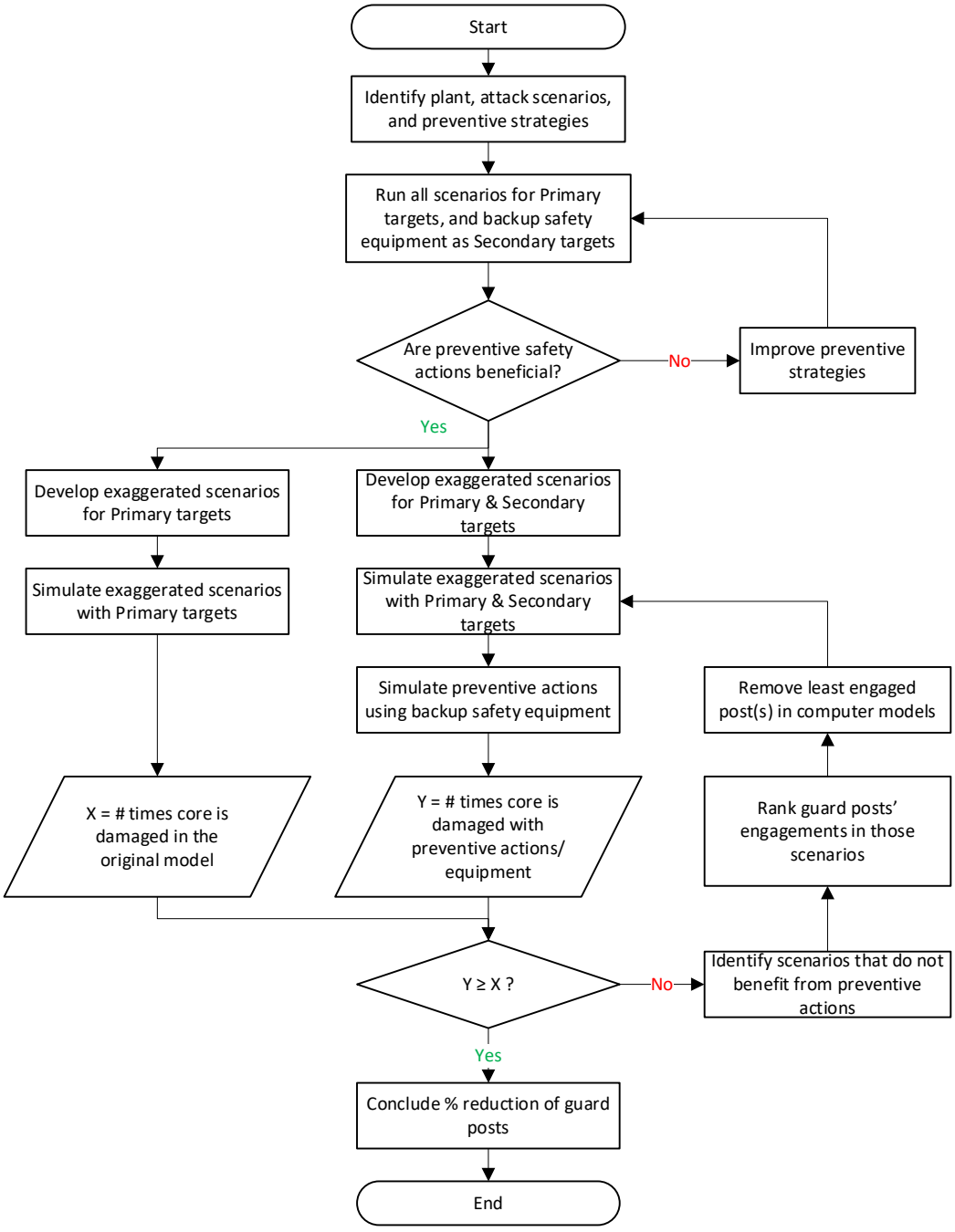

Figure 1. Methodology flowchart

The next step in the methodology is to develop exaggerated scenarios to provide sufficient computational perturbations to most of the guard posts in the model. This process is described further in the next subsection. The exaggerated scenarios are developed for the baseline model consisting of primary targets only, and for the modified model that has both primary and secondary targets. Primary targets refer to the initial design-basis systems and components, while secondary targets refer to additional equipment beyond primary targets to be used in the preventive safety actions, such as FLEX pumps. Simulations are run for both models. As described previously, a loss of these target sets always leads to the core damage event in the conventional analysis method. However, we take the analysis a step

further by simulating preventive safety actions using backup safety equipment. The hypothesis is that there should be fewer core damage events observed than the conventional analysis' results. This reduction in core damage likelihood due to preventive safety actions provides some additional margin to be credited to the plant's resilience to sabotage attacks.

The added security margin is capitalized to relax the PPS requirements by reducing the number of guard posts iteratively. The guard reduction process in this case study is refined from what was done in our previous work [5]. While the previous work analyzed all simulation results to identify the least engaged guard post, this work uses only a subset of the results. The attack scenarios are classified into the post reduction set and the validation set. The post reduction set contains scenarios that do not benefit from the preventive actions, while the validation set has the remaining scenarios. Results in the post reduction set are used to rank the guard posts' engagement according to the number of times they neutralize adversaries. The purpose of using this reduced set of results is twofold: 1) To focus the analysis on relevant data where physical protection does not enable prevention of core damage, and to screen out irrelevant data where physical protection does enable core damage prevention using the NPP's potential safety capabilities; and 2) To shorten the computational complexity. One or more less engaged posts are then removed from the physical security model. The model is simulated again using attack scenarios in the validation set. The purpose this time is to validate that the modification still allows the added benefits of safety actions. If the safety actions are still beneficial, the next less engaged guard(s) can be removed, and the validation step is repeated. The ratio of guard posts in the final security posture to the initial posture informs the percentage of guard posts reduction.

Further details describing the modeling tools in this methodology are given in the following subsections.

2.1 Physical Security Analysis Tool: Simajin

The comprehensive physical security plan of a nuclear facility is evaluated both by the facility itself and the NRC and tested through exercises. It is costly, and often impractical, to evaluate the security plan through actual field exercises. Therefore, computer modeling and simulation are often preferred for this evaluation. There are several third-party physical security simulation tools available, such as Sandia National Laboratory's Scribe3D [6], RhinoCorp's Simajin [7], and ARES's AVERT [8] software tools.

This work uses Simajin tool to simulate and analyze sabotage attacks. Simajin is a three-dimensional combat simulation commercial software. Simajin provides users an ability to determine risk associated with physical security processes using modeling and simulation. The physical security simulation tool enables physical security analysis across a range of environments and with any number of threat vectors and variables. The features enable analysts to conduct risk assessments and quantify how well a protective measure will repel, or defeat, a suite of tailored threats. It is licensed and used in the U.S. DOE and NRC marketplace for the probability of neutralization computations.

Nuclear power plants usually have a good level of security to intercept and neutralize security attacks swiftly, even while adversaries are still at the perimeter fence. Unfortunately, this situation makes it difficult to assess the effectiveness of guard posts located deep within the plant. For that reason, exaggerated scenarios which overestimate the adversaries' capabilities or underestimate the responders' capabilities are generated. They allow security simulations where the adversaries intrude significantly deep within the facility such that all guard posts respond to the attack and therefore the posts' performance can be evaluated and ranked. Although there are no specific acceptance criteria on what can be considered as a good exaggeration to an attack scenario, a practical rule of thumb is to improve the adversary capabilities such that the adversaries are successful in about half of the number of attacks they carry out. Of course, such an exaggeration is far from realistic, yet it is useful to achieve the type of analysis required in this work. In Simajin, such an exaggeration can be done by increasing the number of adversaries, increasing adversaries' probability of hit and kill numbers, decreasing the responders'

probability of hit and kill numbers, decreasing the sensors' detection probabilities, or a combination of these techniques as described in [9].

2.2 Safety Analysis Tool: MAAP

This work credits safety actions that can be done to prevent the release of radionuclides in the event of a sabotage attack. These actions may be done before or after the attack is completed. The safety actions depend on the sabotaged targets and the timing of the sabotage. There are uncertainties in the effectiveness of these safety actions due to the dynamic and uncertain nature of the attack's progression. For that reason, these safety actions need to be simulated together with the physical security simulation. This simulation is done using reactor safety analysis tools, such as RELAP5-3D [10], Modular Accident Analysis Program (MAAP) [11], MELCOR [12], etc.

This work uses MAAP as the safety analysis tool. MAAP is a thermal-hydraulics tool developed by the Electric Power Research Institute (EPRI) to predict plant responses to upset events, including severe accident phenomena. It also tracks the transport of energy and mass, accounting for inventories of water, hydrogen, aerosols, and radioactive species. It uses predetermined values to reduce some of the calculations to algebraic expressions, which makes the calculation time 10 to 100 times faster than MELCOR. However, the predetermined values may limit the flexibility of the model to within given boundaries.

As with the other thermal-hydraulics codes, MAAP can be used to provide a more precise determination of CD, given specific component failure times. The software is available to EPRI members.

2.3 Dynamic Simulation Tool EMRALD

Idaho National Laboratory (INL) developed EMRALD [13], a dynamic probabilistic risk assessment (PRA) tool. This tool has two main components: the model development module, which is hosted online at https://emraldapp.inl.gov and the model solver module that can be downloaded from the EMRALD site. EMRALD plays a key role in the MASS-DEF framework since it can couple the physical security analysis tool and the MAAP safety analysis model with dynamic operator actions modeled in EMRALD. Depending on the outcome of physical security simulations, EMRALD can simulate preventive safety actions and their uncertainties, feed the outcome of those actions to MAAP, and fetch MAAP's results.

EMRALD also contains traditional PRA elements such as fault trees, failure rates, and failure probabilities. Therefore, EMRALD can estimate random component failures, and even human failures, during the preventive safety actions. This capability allows the simulation to be more realistic.

3. PLANT-SPECIFIC MODEL

Each nuclear facility determines the most probable set of attack scenarios for the facility. This is done by finding what component sets if removed from service would cause CD and evaluating different physical attack paths using tabletop exercises, simulation, and FOF drills.

An NPP collaborated on this research and provided access to their attack scenarios, physical security analysis models, plant procedure data, and thermal-hydraulics model. All of this was used in the modeling and evaluation of using operator actions and physical equipment as prevention methods for their scenarios. This is a research project and meant to follow a full modeling and simulation evaluation process for an actual NPP; while the results could be used for as information for an actual plant modification the plant, that was not the goal. The goal was to evaluate the process and find any issues or improvement areas.

3.1 General Information of the Plant

This subsection describes some general information on the collaborating NPP. Using the attack scenarios provided by the NPP, scenarios were evaluated to determine prevention options. The main idea was to use existing mobile backup equipment such as FLEX equipment, cooling pumps or generators, to prevent scenarios from going to CD and to these equipment, hookups, and water sources as additional targets in the target sets of the scenarios. Procedures for retrieving and hooking up the backup equipment were gathered with the time estimates for each of the tasks. Scenarios were evaluated to determine which ones would benefit from backup equipment. It was determined each scenario that could benefit from backup equipment could use a cooling pump to add water to the secondary cooling side.

Typically, an "all clear" status that signals the threat has been neutralized needs to be achieved before plant operators can perform safety tasks on the field. Unfortunately, it can take a long time to perform an extensive security sweep throughout the facility to confirm the "all clear" status. In situations where immediate actions need to be taken to prevent CD, operators can be escorted to their work locations by armed guards in this particular NPP after a security sweep of select areas is done. The sweep procedure and time varies among nuclear plants and may also vary by the attack. In light of such uncertainties, this work assumes a conservative sweep time. Nuclear plant analysts may update this conservative sweep time with their plant-specific data if needed.

FLEX equipment in this NPP is stored in a remote building such that it requires a considerable time to retrieve and set it up. The total time required to perform the security sweep and to retrieve FLEX equipment is often more than the available time window to prevent the core damage following an incident. Therefore, in many cases, FLEX equipment may not be helpful to prevent core damage following a sabotage attack. For that reason, some strategies should be developed to allow the use of FLEX equipment. For example, the equipment may be pre-staged at or near their operational location. Experts at the NPP have also suggested to fill steam generators with supply water at the start of an attack to prolong the design basis decay heat removal time before additional operator actions are needed. Hypothetical procedures were developed to initiate filling the steam generators up to 80% capacity when the main control room is notified of an attack.

While filling the steam generators provides additional time for FLEX implementation, the requirements of NRC Regulatory Guide (RG) 5.81 for target set identification would not allow credit for a pump stored outside of the protected area. To move the FLEX storage location to within the protected area (PA) would be exceedingly expensive and difficult due to the technical requirements for FLEX storage building and the lack of space in this NPP. In some situations, a piece of FLEX equipment could be pre-staged in a semi-permanent location inside the PA, as long as it meets the storage location requirements which could be cost or space prohibitive. With such considerations, the NPP staff proposed to consider a "Security Response Pump" as an alternative to FLEX pumps. This pump would be identical to the FLEX pump in capability, procedures, and connections but would be dedicated for use in security responses.

Data for determining time distributions for tasks in the model were obtained from either training exercises, expert judgment, or a combination of the two, depending on the level of data available from the NPP.

3.2 Physical Security Analysis Model

An existing Vanguard/Simajin model for the collaborating NPP was used as the starting point for this work. The model itself is not described in this report because it is classified as SGI. The model is used as the starting point for an initial testing as described in Section 2. It was then modified to include exaggerated scenarios and used in iterative simulations following the flowchart in Figure 1.

3.3 MAAP Model

A thermal-hydraulic analysis of the nuclear plant is needed to determine if or when core damage occurs following a sabotage attack. The model for this analysis should include parameters to adjust data related to the attack and preventive actions, such as the loss of cooling options, the inclusion of backup cooling through FLEX or security pumps, and the timing of those events. For this case study, our collaborating plant provided a MAAP model along with an input file to specify key component failure time such as the timing when pumps are destroyed, or external pumps start. Because they wanted to evaluate filling the steam generator during an attack, they also modified the MAAP input file to include a start and end time for the filling activity. The MAAP input file uses input blocks to evaluate the current time against a specified time to trigger the filling, cooling, and backup pump conditions; Figure 2 highlights the value to modify to set the time for the auxiliary feed pump to activate. The EMRALD model is built such that it can modify this input file and write the timing data according to the times they occur in the EMRALD simulation.

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

Figure 2. Example of MAAP input block to set the motor-driven pump to fill the steam generator starting at time 0.

3.4 EMRALD Model

A generic pressurized-water reactor (PWR) EMRALD model was developed and used as the basis for this work. A detailed report outlining the model pieces and functions will be released at the end of the fiscal year 2023. The generic model does not have any target sets or safeguards information (SGI) but has common components that could be targeted in an attack. Some plant-specific information such as timing data may need to be added to make the analysis more realistic, however it would make the model SGI.

3.4.1 Model Development

The development of the generic EMRALD model was done in a normal office space because the generic model does not contain any proprietary information that requires any safeguards procedures. An NPP can acquire this generic model and fine-tune it to match their plant-specific data in a secure working environment. For example, the generic model includes two motor-driven auxiliary feed water pumps and two steam-driven pumps by default. If a facility does not have any auxiliary feed water pump, they can simply disable these pump modules in the model.

Generic operator actions are included in the EMRALD model without any proprietary or plant-specific information either. Any plant-specific procedures may be added once the model enters the SGI space. For this case study, the plant personnel suggested that we add a procedure to fill the steam generator up to 80% when an attack has been announced. This strategy could provide additional time before core is damaged.

Finally, we set up the prevention actions to be done after an attack. Options included in the generic model include manual operation of the turbine-driven pumps, fire water, a staged protection pump, fire truck, and FLEX pump. In this study, we simulated the manual turbine-driven auxiliary pump operation.

3.4.2 Model Simulation

Modifications to and simulations of the generic model with plant-specific information were done following applicable regulations on SGI. This subsection describes general practices used to perform this process, excluding the SGI data and information.

In order for EMRALD to receive data from the Simajin simulation results, EMRALD variables must be designed with names that correspond to the variables in the Simajin results as shown in Figure 3 below. Therefore, the variable names for breach or sabotage times in the EMRALD model were designed to match the Simajin models.

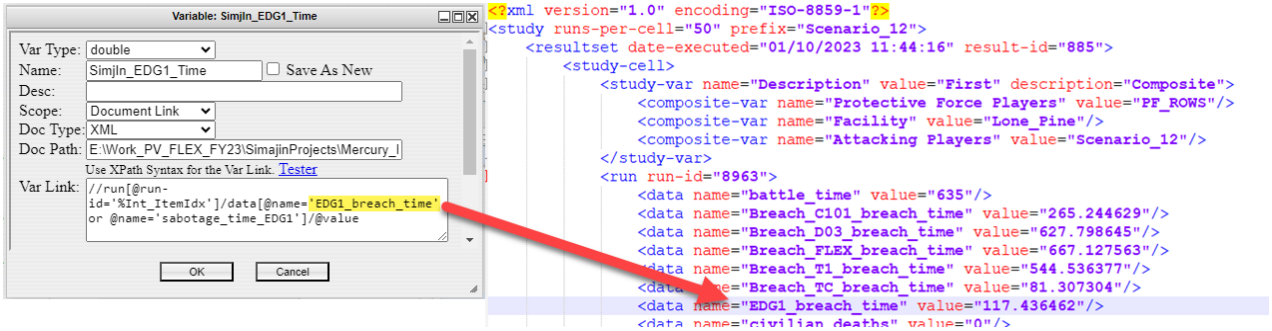

Figure 3. Left: EMRALD variable for electric diesel generator attacked time. Right: Simajin results for the sabotage time. Variable names between the two models must match.

The EMRALD model with properly designed variables was simulated, reading the target set results from the SIMAJIN model and running MAAP as shown in Figure 4. Each of the physical security scenario simulation results were used by EMRALD to determine how much time the operator had to fill the steam generator, if the "after attack" prevention options worked for targets hit, and MAAP was used to evaluate the combinations and timing for CD.

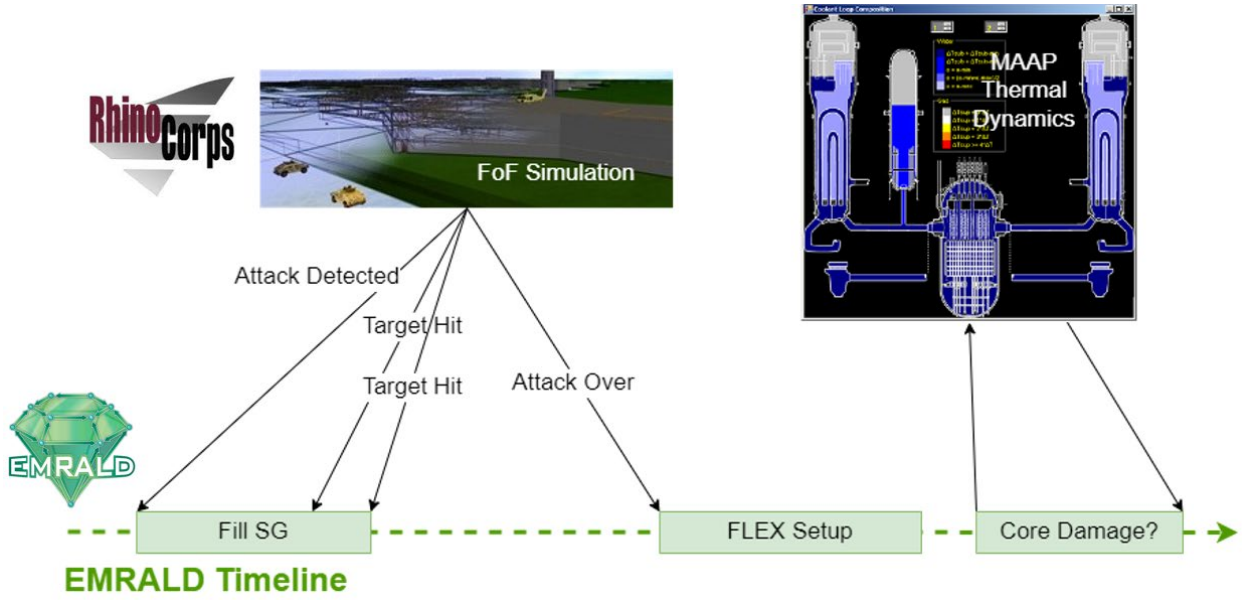

Figure 4. Data and interactions between the tools used.

4. RESULTS AND DISCUSSIONS

4.1.1 Initial Preventive Strategies

Six significant attack scenarios were selected to modify preventive safety actions using FLEX equipment following a sabotage attack. Exaggerated cases of these six scenarios were created by modifying the hit-to-kill probabilities and increasing the number of adversaries in the Simajin models.

Simulation results of these attack scenarios are shown in Figure 5. By comparing the simulation results, we can see the potential benefit of preventive safety actions that can be capitalized in the guard reduction process. The second column in the figure informs the reduction of attack success when preventive actions are done, relative to without preventive actions. This column shows that scenarios S3 and S6 benefit from the safety action strategies because the adversaries' success likelihood is reduced considerably. As such, these two scenarios are categorized as "Good Reduction". On the contrary, safety strategies in scenarios S1 and S2 reduce attack success likelihood only slightly. However, the usefulness of safety strategies in these scenarios can be improved. The limiting factor for scenarios S1 and S2 was the insufficient time for operators to retrieve and set up FLEX equipment to perform the safety actions. If the equipment was pre-staged or stored closer, they could provide a significant benefit as shown in the third column. For that reason, these scenarios are categorized as "Could be good". In the last two scenarios, S4 and S5, the backup safety equipment was easily hit along with the initial targets; and therefore did not impede adversary attacks significantly. Improvements need to be made to protect the backup equipment for them to be beneficial in preventing core damage in these scenarios. Therefore, the safety strategies in these scenarios are categorized as "Needing Protection". Before continuing with the next step, the safety actions should be improved so that they provide a benefit to a significant number of scenarios.

Scenario	Reduction in Adversary Success Rate	
	Reduced attack success % with current FLEX setup	Maximum reduction with optimal staging*
S1	3%	56%
S2	13%	55%
S3	73%	75%
S4	14%	14%
S5	4%	4%
S6	63%	63%

Could be good

Needs Protection

Good Reduction

*With reduced time in obtaining cooling (i.e., closer flex, pre-staged, and protected)

Figure 5. Reduction of adversary success rate when including the FLEX pump.

4.1.2 Improved Preventive Strategies

The collaborating NPP provided feedback after receiving the initial results of this study. They were in the process of making some security changes that would alter some guard positions and timing data, so the model was modified to incorporate those new changes. They also commented that it is not ideal to use FLEX equipment for security response purposes due to practical constraints from regulatory requirements for both the usage and location of FLEX equipment. For that reason, it was decided to use a FLEX-like pump called a "Physical Security Response Pump" by modelling it staged inside the Protected Area (PA). This approach reduces the time needed to retrieve and set up the pump significantly. In addition, it eliminates the need to meet all the requirements and overhead of an actual FLEX pump for external hazards. Finally, an additional location for a pump connection to the secondary cooling was added to the model. This strategic location is more easily protected from an adversary attack, with the intent to allow enough time for the security protection pump to be used. The security pump was also added to the attack scenarios as a Secondary target in Simajin, by inserting it in adversaries' path of disabling the primary targets where applicable.

4.1.3 Guard Post Reduction

After the preventive safety actions were modified, a comprehensive evaluation of all scenarios was conducted where the results were analyzed following the approach in Section 2. The physical security and EMRALD models were modified to include actions using security pump in these identified scenarios. Exaggerated scenarios were created for all the scenarios and were included in the evaluation.

Physical security simulation results from the exaggerated scenarios are listed on the second column of Table 1. This column lists the likelihood of adversary success in sabotaging the targets in their initial attack plan. As the Table shows, the scenarios satisfy the rule of thumb for exaggerated scenarios described in Section 2.1. After the security pump is added into the scenarios as the adversaries' secondary target, a quick evaluation of potential benefits can be done by comparing adversaries' success rates between primary targets and both primary and secondary targets. This is shown in columns 2 and 3 of Table 1, where values in column 3 are significantly less than the success rate to sabotage the primary targets only for most scenarios. Not all results are shown in this Table, however it can be said that about half of all scenarios could benefit from the use of a security pump. This shows the maximum potential benefit if the safety actions can be performed in time.

Table 1. Comparison showing a few of the exaggerated scenario's results with added targets and EMRALD simulation results.

Scenario	Adversary success likelihood	
	In sabotaging Primary targets	In sabotaging Primary and Secondary targets
A	51.2%	2%
B	68.4%	11.2%
C	52%	13.2%
…	…	…
Y	26.4%	25.2%
Z	71.6%	34%

The physical security simulation timing information was then used to run the EMRALD model simulating the safety actions and a time-specific thermal hydraulic analysis. These simulations determine if there is core damage or not given all the timing information. These results are listed and compared in Table 2. The first column indicates the core damage likelihood in the conventional analysis method, that directly corresponds to the adversaries' success likelihood in sabotaging the Primary targets. Meanwhile the second column shows the core damage likelihood when preventive safety actions are taken following a successful sabotage attack. The reduced numbers in this second column indicate the added security margin from crediting prevention strategy modeled in EMRALD. This observation confirms the hypothesis that the NPP is actually more robust to sabotage attacks than what was previously assumed during the initial design of the physical protection system (PPS). As a result, the conservatism in the initial PPS strategy can be modified without sacrificing its safety objective, by reducing the number of guard posts in this case.

Table 2. Comparison showing a few of the exaggerated scenario's results with added targets and EMRALD simulation results.

Scenario	Core damage likelihood	
	Without preventive safety actions	With preventive safety actions modeled in EMRALD
A	51.2%	4%
B	68.4%	13.4%
C	52%	14.4%

…	…	…
Y	26.4%	25.2%
Z	71.6%	37.6%

Results showed that the addition of Secondary targets and prevention actions successfully reduced the adversaries' success likelihood by over half for almost all scenarios. As explained in Section 2, the results are used to classify scenarios into the post reduction set and the validation set. Analysis from the post reduction set reveals that there are several guard posts with no or little engagement in stopping adversaries. One or more of them were then removed from the exaggerated scenarios iteratively, while retaining posts that contributed to stopping adversaries from sabotaging the secondary targets.

In the end, it was concluded that 22% of the guard posts in this NPP could be removed without compromising the physical security objective of preventing the core damage. This reduction was made possible by crediting preventive safety actions using backup equipment in the analysis. As a note, the reduction was made by merely removing the posts without reorganizing their locations. Further reductions may possibly be pursued if the guard post locations are strategically repositioned to recompense the lost posts and to provide better protection against sabotage attacks.

5. SUMMARY AND FUTURE WORK

This report documents further progress on continuing work within the LWRS program's physical security pathway to develop methods and tools to support the optimization of physical security postures using modeling and simulation. Previous studies developed MASS-DEF as a dynamic computational framework that links results from commercially available FOF simulation tools, commercially available thermal-hydraulic tools, and the dynamic risk modeling tool EMRALD to model the complex nature of physical security scenarios and the time dependent nature of how CD could occur during these scenarios more accurately. Previous studies also 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 a previous report, the MASS-DEF process was applied to an actual commercial NPP to verify that results obtained using generic models represented actual scenarios and to further refine the guidance to support future analysis by other utilities. As part of previous research, a generic EMRALD model was developed to reduce the modeling effort that a utility would need to perform to replicate this type of analysis. In this analysis, reasonable results were obtained, and several valuable insights about the potential effectiveness of crediting backup safety equipment in security scenarios were identified. Feedback from the utility regarding both the process and the analysis of the results was obtained. In this study, modifications were made to the plant FOF model to implement a "Physical Security Response Pump." This pump is identical to the plant FLEX pump but would be pre-staged inside the plant's protected area and include physical security delay features to reduce the ease of sabotage. Additionally, the placement of guard positions was evaluated to maximize the benefits of crediting this additional pump. 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. Additionally, the data created through this phase of analysis will be used to identify potential post reductions that could be reasonably justified by including the physical security response pump into the security plan. These post reductions will then need to be analyzed for overall potential cost savings compared to the cost to implement the changes including purchasing equipment, training staff, installing additional delay features, engineering analysis, and regulatory issues related to changes in the physical security plan.

A licensee could adopt the MASS-DEF process to explore and implement an updated or optimized physical security plan (PSP) while meeting the existing NRC regulations. Figure 6 illustrates the different

NRC regulations that a licensee could consider while updating their PSP. Within 10 CFR 73.55(r), the NRC may authorize a licensee to implement alternative measures of protection against radiological sabotage. A licensee may consider updating its PSP to incorporate additional security features such as security technologies or operator actions to reduce the number of armed guards (Figure 6). If, in a rare instance, the updated PSP does not meet the existing regulatory requirement (say, of minimum number of armed guards), then a licensee may consider implementing the updated PSP by requesting an NRC exemption under 10 CFR 73.5. It is likely that the updated PSP would meet the existing regulatory requirements in which case a licensee should then check if the effectiveness of the updated PSP is less than that of the current PSP. The flowchart in Figure 7 describes in detail the process for a licensee to implement the MASS-DEFF process to calculate the effectiveness of their current and updated PSP and to follow the possible regulatory paths. If the effectiveness of updated PSP is less than the current PSP, then the licensee may consider filing a license amendment request under 10 CFR 50.90 before implementing the updates (Figure 6). When the effectiveness of the updated PSP is not less than that of current PSP then the license may implement the changes and report to NRC as per 10 CFR 50.54(p)(2) (Figure 6).

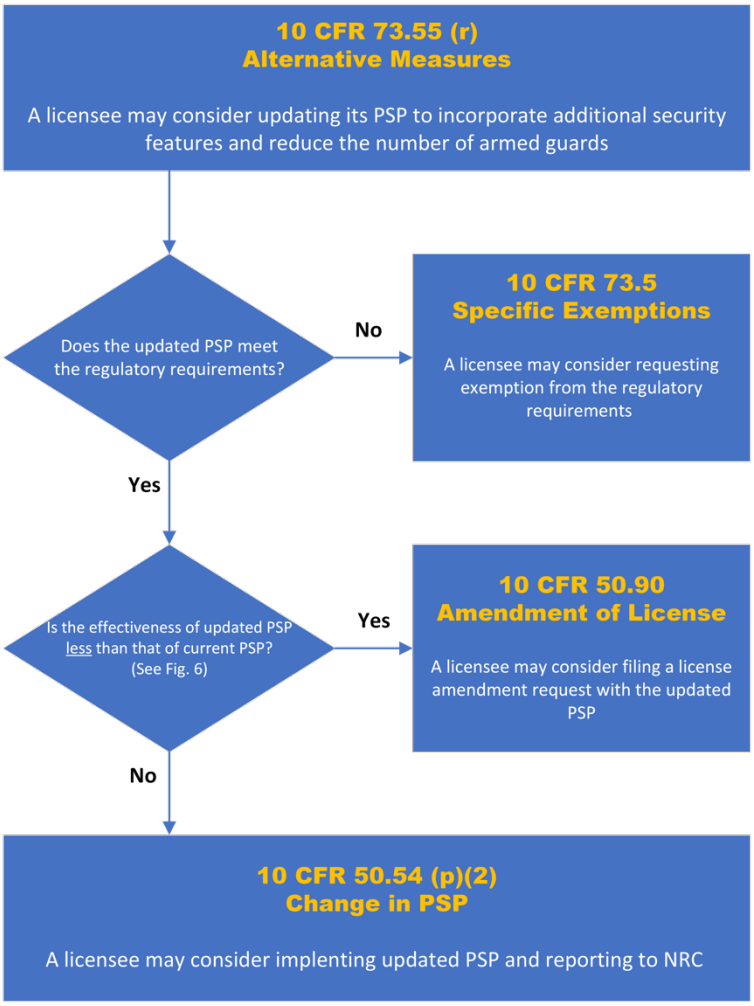

Figure 6. The different NRC regulations a licensee could consider for their updated physical security plan.

The flowchart in Figure 7 illustrates some simplified steps of implementing the MASS-DEFF process by a licensee. The process starts by calculating the effectiveness of a plant's current PSP using MASS-DEFF process. The flowchart shows several key steps in identifying potential changes in PSP through the plant's internal review and vetting process by a team of plant's experts in security, safety, and operations.

The approved changes in plant's PSP will result in an update PSP for which MASS-DEFF can be used to calculate the effectiveness. Based on the outcome of MASS-DEFF process for the updated PSP, the flowchart (Figure 7) then describes the key steps of regulatory process a licensee may consider to adopt.

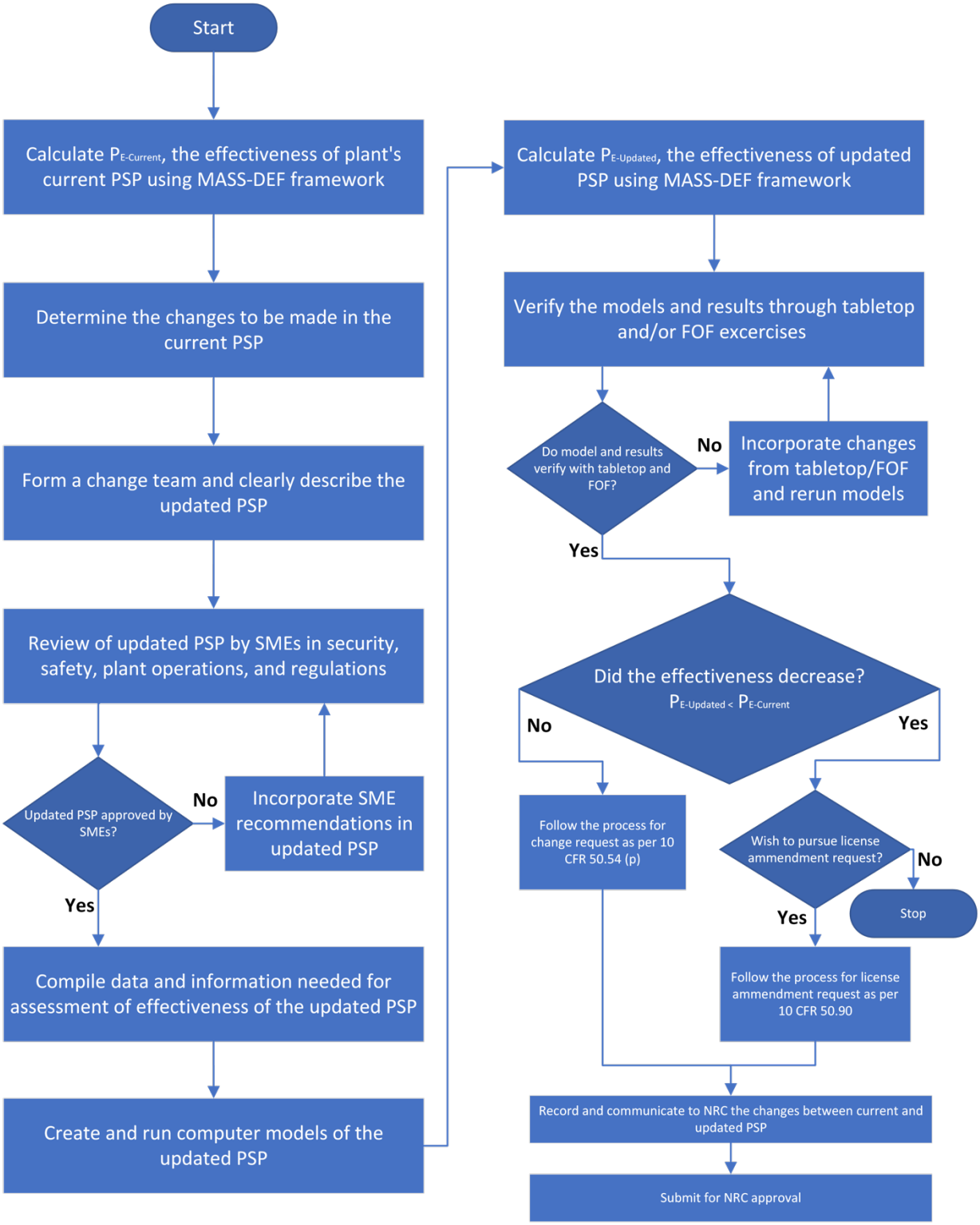

Figure 7. Flowchart for PSP effectiveness evaluation for regulatory considerations.

5.1 Hypothetical Next Steps for the NPP

As emphasized earlier, this research was done to evaluate and test the ability to use modeling and simulation to numerically evaluate other strategies in preventing CD for physical security scenarios. This work was done with actual NPP scenarios and data. Although the NPP did not express any immediate plan to modify their PPS following the results from this study, the follow up steps are summarized in this Section.

This methodology would produce a technical basis for the proposed changes. The technical basis would show an equivalent or improved security performance, and as such, the change would comply with:

- the 50.54(p)(2) for changes to security plans
- the 73.55(r) pending a cost analysis consistent with 73.55(r)(4)(iii).

The change may also fall under the requirements of a license change as defined by 50.54(p)(1). License change justifications would follow a similar process to 50.54(p)(2) but would follow different submission and approval requirements from the NRC. Postulated changes that fall outside the prescriptive requirements found in 10 CFR 73.55 would require an exemption request approval consistent with 10 CFR 73.55.

The process to use the methodology and justify the results for a 50.54(p) change are outlined as:

1. Form a technical team to perform analysis following the methodology described in Section 2
2. Review scenario(s) to be included in the simulations by subject-matter experts
3. Compile data for the baseline and exaggerated scenarios
4. Follow MODSIM iterative process: preparation, model baseline, model changes, run simulation, compare to base case, iterate process to achieve desired results
5. Verify MODSIM results with tabletop/FOF exercises (NRC may wish to observe these processes)
6. Review the PPS' compliance with 50.54(p) requirements (above minimum, etc.)
7. Compile documentation required by 50.54(p), 50.90, or 73.55(r), following NEI 11-08 guidance [14]
8. Draft implementation provisions (site procedures, etc.)
9. Record changes (e.g., draft security plan changes)
10. Transmit documents to NRC for feedback
11. Notify NRC of the changes, or submit an application for approval, following NRC's guidance in the previous step.

The report summarizing the proposed change should include the following documentation:

- Security plan change report (follows NEI 11-08 criteria and format)
- FOF exercise/tabletop verification results
  - Removal and/or reconfiguration of guard posts
  - Preventive safety actions after security attacks
- Limited scope performance testing results

- Drafts of site procedure updates
- Draft of security plan updates
- Any other pertinent documentation.

The NPP could gain significant cost savings by applying the guard post reduction methodology and using the results to demonstrate regulatory compliance to the NRC. While an exact cost-saving dollar amount cannot be stated in this report, it would be equivalent to the cost and overhead for 22% of the response force currently at the facility. Each post consists of more than 3 employees, each of whom can cost a facility between $500-900K a year.

REFERENCES

1. PG&E. 2018. "PG&E Company 2018 Nuclear Decommissioning Cost Triennial Proceeding Prepared Testimony – Volume 1." 18-12 (U 39 E), Pacific Gas and Electric Company. https://analysis.nuclearenergyinsider.com/pge-seeks-decommissioning-head-start-cost-estimates-rise.
2. U.S. NRC. 2020. "Emergency Preparedness in Response to Terrorism." About Emergency Preparedness, U.S. Nuclear Regulatory Commission. Last modified Nov. 13, 2020. https://www.nrc.gov/about-nrc/emerg-preparedness/about-emerg-preparedness/response-terrorism.html#one.
3. U.S. NRC. 2021. "PART 73—Physical Protection of Plants and Materials." (NRC, 10 CFR), U.S. Nuclear Regulatory Commission. Last modified Mar. 24, 2021. https://www.nrc.gov/reading-rm/doc-collections/cfr/part073.
4. NEI. 2016. "Diverse and Flexible Coping Strategies (FLEX) Implementation Guide." NEI 12-06, Rev. 4, Nuclear Energy Institute. https://www.nrc.gov/docs/ML1635/ML16354B421.pdf.
5. Christian, R., S. R. Prescott, V. Yadav, S. St. Germain, C. P. Chwasz. 2022. "Evaluation of Physical Security Risk for Potential Implementation of FLEX using Dynamic Simulation Methods." INL/RPT 22 70315, Rev. 0, Idaho National Laboratory, Idaho Falls, ID. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_64424.pdf.
6. SNL. n.d. "Scribe3D." Sandia National Laboratory, National Technology and Engineering Solutions of Sandia, LLC, *Sandia INSE Tools*. Accessed Jun. 15, 2023. https://insetools.sandia.gov/scribe3d.
7. RhinoCorps. 2021. "Rhino Corps Homepage." *RhinoCorps Ltd. Co*. Accessed Jul. 28, 2021. https://www.rhinocorps.com.
8. ARES. 2022. "AVERT Suite." *ARES Security*. Accessed Nov. 14, 2022. https://aressecuritycorp.com/software/avert-suite.
9. Christian, R., 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* **197**, no. 1 (2022): pp. S24 S44. https://doi.org/10.1080/00295639.2022.2112899.
10. INL. n.d. "RELAP5-3D." Idaho National Laboratory, Idaho Falls, ID. Accessed Jun. 15, 2023. https://relap53d.inl.gov/SitePages/Home.aspx.
11. EPRI. 2012. "Modular Accident Analysis Program." Brochure 1025795, Electric Power Research Institute, p. 4. Accessed Jun. 15, 2023. https://www.epri.com/research/products/000000000001025795.

12. SNL. n.d. “MELCOR.” Sandia National Laboratory, National Technology and Engineering Solutions of Sandia, LLC, *Sandia Energy*. Accessed Jun. 15, 2023. https://energy.sandia.gov/programs/nuclear-energy/nuclear-energy-safety-security/melcor/.
13. INL. n.d. “EMRALD.” Idaho National Laboratory, Idaho Falls, ID. Accessed Jul. 28, 2021. https://emrald.inl.gov/SitePages/Overview.aspx.
14. NEI, “NEI 11-08: Guidance on Submitting Security Plan Changes”, Nuclear Energy Institute, Washington DC, 2012. https://www.nrc.gov/docs/ML1215/ML12159A388.pdf.