INL/EXT-20-59891

Light Water Reactor Sustainability Program

Methodology and Application of Physical Security Effectiveness Based on Dynamic Force-on-Force Modeling

September 2020

U.S. Department of Energy

Office of Nuclear Energy

INL/EXT-20-59891

Methodology and Application of Physical Security Effectiveness Based on Dynamic Force-on-Force Modeling

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

September 2020

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

ABSTRACT

This report describes the research and development being performed at INL towards a dynamic modeling and simulation framework to enable physical security optimization at commercial nuclear power plants. The framework is based on the dynamic modeling tool EMRALD and is demonstrated for applications that can result in physical security optimization. Two main applications are presented: 1. Integrating FLEX portable equipment performance with force-on-force (FoF)models of a plant's physical security posture, and 2. Location optimization of bullet resistant enclosure.

The generic framework for modeling FLEX portable equipment is described in detail, followed by a case study modeling an adversarial attack aimed at causing a radiological release by sabotaging the plant's power supply and its ultimate heat sink capabilities at a hypothetical pressurized-water reactor. Two distinct FLEX deployment strategies, series and parallel, are modeled with distinct timelines. The results of the adversarial attack modeled in a commercial FOF tool, AVERT, are integrated with the FLEX deployment model in EMRALD. Monte Carlo simulation is used to model the distribution of the timeline in FLEX deployment strategies. Thermal-hydraulic analysis of FLEX performance is performed in RELAP5 and integrated with the EMRALD simulations to provide more realistic timelines in the models. The results demonstrate that, even in the extreme case of a successful adversarial attack, deployment of FLEX equipment can result in a significantly high likelihood of preventing radiological release. The modeling and simulation framework of integrating FLEX equipment with FOF models enables the NPPs to credit FLEX portable equipment in the plant security posture, resulting in an efficient and optimized physical security.

The objective of location optimization of bullet resistant enclosure (BRE) is to determine the best location in the plant for a new BRE being planned by the plant to enhance their physical security effectiveness. The plant physical security FOF model is integrated with EMRALD that performs Monte Carlo simulation to run different attack scenarios and a discrete set of potential BRE locations. Sensitivity analysis is used to determine the most effective location for the BRE. The optimization approach can be extended to wide applications such as location optimization of remotely operated weapons and other strategic fixed assets.

CONTENTS

FIGURES

TABLES

ACRONYMS

AC	alternating current
AFW	auxiliary feedwater
BRE	bullet resistant enclosure
CD	core damage
DBT	design basis threat
DC	direct current
DG	diesel generators
DHS	department of homeland security
DID	defense-in-depth
DOE	department of energy
EDG	emergency diesel generator
ELAP	extended loss-of-ac-power
EMP	electrical magnetic pulse
EMRALD	Event Modeling Risk Assessment using Linked Diagrams
EPRI	Electric Power Research Institute
EUCG	electric utility cost group
FOF	force-on-force
ICONS	International Conference on Neuromorphic Systems
IDS	intrusion detection system
INL	Idaho National Laboratory
LOOP	loss-of-offsite-power
LWRS	Light Water Reactor Sustainability
NEI	Nuclear Energy Institute
NNSA	National Nuclear Security Administration
NPP	nuclear power plants
NRC	Nuclear Regulatory Commission
O&M	operation and management
ORNL	Oakridge National Laboratory
PCT	peak cladding temperature
PPS	physical protection system
PRA	probabilistic risk assessment
PSP	physical security pathway
PWR	pressurized-water reactor

RISA	risk-informed systems analysis
ROWS	remotely operated weapons system
SAFER	strategic alliance for FLEX emergency response
SBO	station blackout
SG	steam generator
SME	subject matter expert
SNL	Sandia National Laboratory
SOCA	Security Fence Owner Controlled Area
STP	South Texas Project
TDP	turbine driven pump
TPPS	Timeline Physical Protection System
TVA	Tennessee Valley Authority
UAO	Unattended Openings
UAS	unmanned aircraft systems

METHODOLOGY AND APPLICATION OF PHYSICAL SECURITY EFFECTIVENESS BASED ON DYNAMIC FORCE-ON-FORCE MODELS

1. INTRODUCTION

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

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

The Nuclear Regulatory Commission (NRC) and industry approach to maintaining effective security at a plant includes various security programs, each with its own individual objectives that, when combined, provide a holistic approach to maintaining the effective security of the plant. 10 CFR 73.55(d)(1) states, "The licensee shall establish and maintain a security organization that is designed, staffed, trained, qualified, and equipped to implement the physical protection program in accordance with the requirements of this section" [5]. NRC security requirements for commercial operating nuclear sites increased exponentially following the September 11 terrorist attacks, resulting in a significant increase of onsite response force personnel across the nuclear industry [3]. The plant's response force includes the minimum number of armed responders as required in 10 CFR 73 and security officers tasked with assigned duties, such as stationary observation/surveillance posts, foot-patrol, roving vehicle patrols, compensatory posts, and other duties as required [4].

The nuclear industry needs to pursue an optimized plant security posture that considers efficiencies and innovative technologies to reduce costs while meeting security requirements. The use of FLEX portable equipment in the plant physical security posture has been identified as one area that holds the potential to optimize the security posture and reduce costs. This report describes the modeling and simulating capabilities developed to incorporate the deployment of FLEX with force-on-force (FOF) modeling of a typical physical security posture at a generic light-water reactor plant.

There are several different levels of FOF modeling from simple procedures of adversary and defense force tasks and probabilities to full 3D models with artificial intelligence to determine character paths, detection, and combat [6]. In this research, we focused on using one of the more complex simulation tools, ARES's AVERT [9] software and evaluating what is needed to evaluate and include FLEX equipment and procedures into the model. Section 2 provides an overview of the modeling and simulation approach developed in this work for physical security optimization, Section 3 describes the integration of FLEX equipment with FOF modeling and simulation and presents a case study, followed by a conclusion in Section 4.

1.1 Current Physical Security Posture

While the U.S. commercial nuclear power industry is among the most robust and well-protected critical infrastructures in the world, increased costs of regulation in nuclear security threaten the long-term operation and future of the existing fleets. NRC and industry approach to maintaining effective security at a plant includes various security programs, each with its own individual objectives that, when combined provide a holistic approach to maintaining effective security of the plant. There has been a continued buildup within these various security programs for commercial nuclear power producing what is widely considered to be the most robustly fortified and protected commercial critical infrastructure in the world.

As part of the research within this effort, the cost of physical security at U.S. commercial nuclear power plants were studied. The cost data is obtained from the Electric Utility Cost Group (EUCG), which is a group of energy companies from around the world participating with the objective of sharing information to help individual companies improve their operating, maintenance, and construction performance [15]. In the current effort, a non-disclosure agreement is executed between EUCG and INL enabling EUCG to share proprietary cost data of physical security at U.S. commercial nuclear power plants. The cost data comprises of four parts: 1. Labor cost, 2. Service cost, 3. Material cost, and 4. Others. Due to proprietary nature of the cost data, dollar values of the cost are not published here.

Figure 1 shows the evolution over the last twenty years the percentage contribution of the four costs towards the total cost of physical security at U.S. commercial NPPs. It is interesting to note the rapid increase in the contribution from labor cost since year 2008, indicating the shift of physical security posture towards labor-intensive approach. Labor costs account for more than 60% of the total physical security budget, and its contribution continues to rise.

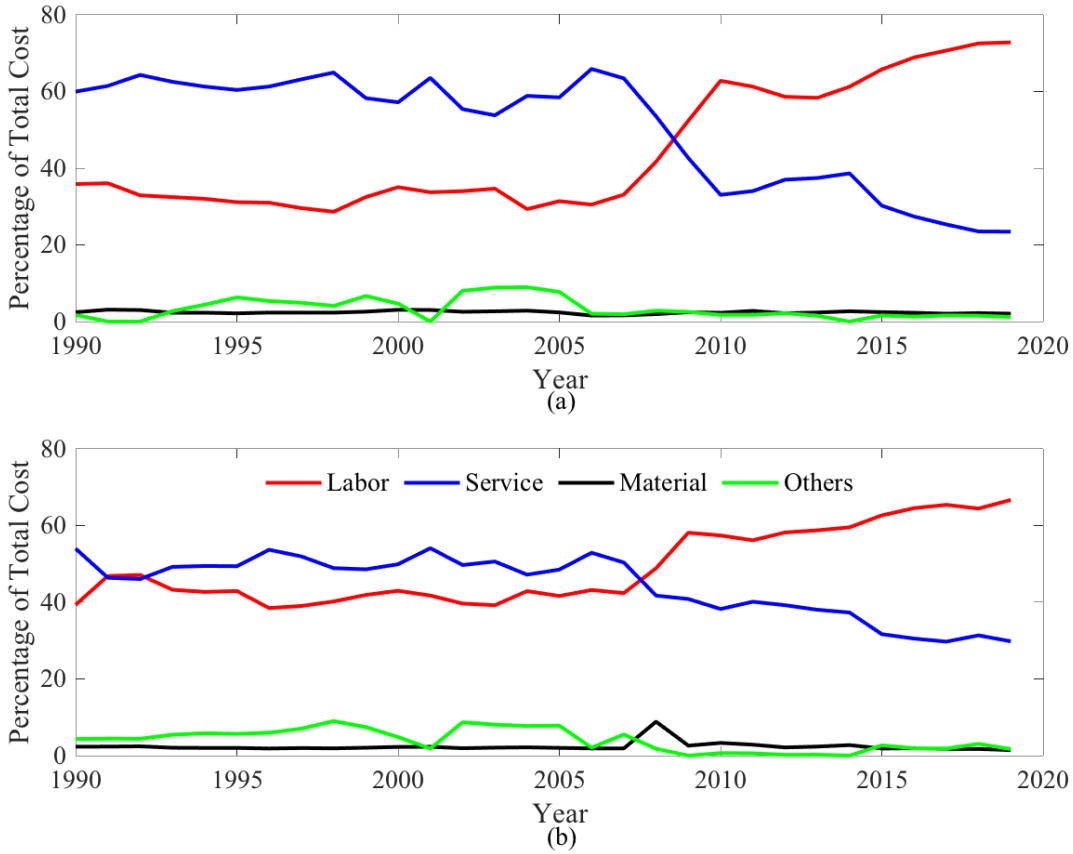


Figure 1. Evolution from 1990 to 2019 of percentage of total cost for the four types of physical security costs: Labor, Service, Material and Others at (a) Single Unit NPPs and (b) Dual Unit NPPs. Notice the continued increase in contribution of labor costs since 2008. Data source: EUCG.

The labor-intensive approach to address the radiological sabotage and theft has come at a very high cost for the nuclear power industry that is extremely difficult to sustain in the current energy situation impacting our electricity generation, particularly in consideration of the recent and announced plant shutdowns the nation has continued to see over the past several years. If commercial nuclear power generation is to be sustained within the United States, an optimized plant physical security posture is needed that will reduce conservatisms in that posture and potentially reduce security costs for the nuclear industry while meeting the requirements of 10 CFR 73 [3].

2. INDUSTRY ENGAGEMENT

This section provides an overview of the engagement of INL research team with the physical security subject matter experts across the industry, vendors, regulators and other national laboratories in form of working group meetings and plant site visits.

2.1 Working Group Meetings

The LWRS physical security working group was established with the objectives of providing stakeholder feedback to the LWRS Program on their research and development needs and priorities, socializing the progress of Physical Security Pathway initiatives, and identifying opportunities for additional engagement and participation of stakeholders in the pathway research activities. The working group also provided a forum for physical security professionals to share common experiences and recommend prioritized activities based on their common needs, discuss the status of ongoing engagement

activities through research and development activities and identify additional engagement and participation opportunities in PSP research activities. This working group is comprised of nuclear enterprise physical security stakeholders and the meeting included over 10 Utilities representing roughly 60 nuclear power plants (NPPs), two staff from the NRC, physical security vendors, the Nuclear Energy Institute (NEI), the Electric Power Research Institute (EPRI), and staff from Sandia National Laboratory (SNL), Idaho National Laboratory (INL), and ORNL. The NRC is an important stakeholder of the LWRS PSP WG and will be invited to participate on the working group.

Three working group meetings were held since September 2019. The meetings had an overwhelming response across the spectrum of stakeholders, and enabled in depth technical discussion and provided the research team with valuable inputs about specific challenges faced by the industry. Appendix A provides the details of the working group meetings.

2.2 Plant Site Visit

Two site visits were conducted at the Monticello Nuclear Generating Plant (initial security site visit and FoF exercise site visit) in FY19, details of which are provided in the joint SNL-INL report [16]. Three site visits were conducted in FY20 to gain a better understand of the differences in general facility layout, security based on the number of plants, leveraging a utility's fleet base, etc.

2.2.1 Palo Verde Visit

INL and SNL representatives visited the Palo Verde NPP to discuss new methods and technology to optimize physical security. The Palo Verde NPP is the largest in the united states and is surrounded by open desert. While the overall goals are the same, the environment makes its security needs, issues, and options different than other facilities. Palo Verde also had their security modeling done by Rhino Corps using their software Simagin.

The plant visit provided the opportunity to examine and discuss previous, existing and future security options as well as review of their dominating target set scenarios. Part of the visit allowed for the reviewing of existing security measures and changes due to inspections or protection strategy. The following are some issues or observations made by the facility:

- Given the large plant footprint and need for easy access between reactors, they have a hard time installing delay barriers effective enough to allow time for relocating protection forces to intercept adversaries.
- Taking credit for early warning of the outer fence or SOCA detection area is difficult due to the maintenance and testing costs of the fence. (1M a year in maintenance).
- They have a couple of dominating scenarios and methods reduce security requirements for those scenarios would have large effect on the security costs.

The following technologies or design options were discussed:

- EMRALD for dynamic modeling to include operator actions or partially damaged equipment scenarios.
- Deliberate motion algorithms with a virtual fence to eliminate much of the perimeter fence requirements.
- Cyber security issues.
- Incorporating FLEX equipment into scenarios.
- Hardening of key crosstie equipment to credit key scenarios.
- Evaluation of SOCA and other equipment testing to reduce maintenance costs.

2.2.2 South Texas Project Visit

South Texas Project (STP) invited INL to visit and discuss options to collaborate a project to incorporate FLEX equipment and equipment optimization for physical security protection strategy. The STP facility is ideally situated due to the pre-staged FLEX equipment and the existing hardened structures around that equipment. INL attendees were able to observe security measures along with the FLEX equipment then discuss the process and needs for incorporate the FLEX procedures into the security modeling. The team performed a detailed site walkdown with security staff. The walkdown included current and potential future post locations as well as the pre-staged FLEX equipment. The team was also able to meet with some members of STPs PRA staff and some familiar with the Thermo-hydraulic modeling of the reactor accident scenarios. STP staff provided valuable insights into potential security related considerations for crediting FLEX equipment as well as some other potential applications of using dynamic physical security simulation methods for optimizing potential security capital upgrade projects.

2.2.3 VC Summer Visit

LWRS staff attended the Virgil C. Summer Nuclear Station NRC Triennial Force-on-Force exercises. LWRS staff observed the triennial drill as guests of the NRC inspection team. The primary purpose of the observation was to identify aspects of the force-on-force exercise drill that might require modification of force-on-force simulations to allow use of simulations to evaluate potential differences between NRC exercise performance and expected actual attack performance. Another purpose of the observation was to further familiarize the LWRS team with scope and effort required to perform an NRC triennial inspection. The visit also provided valuable exposure to additional security postures, tactics and physical security system layouts. The team observed two live exercises as well as the required safety briefings, safety walkdowns and post exercise reviews. One exercise was conducted during daylight hours and another was conducted after dark providing the team with valuable insight into the additional challenges posed to protective forces defending a station at night. Of particular note was the total number of staff required to support the exercises. It was estimated that approximately 80 to 90 plant staff were required to support the exercise, this included drill observers, safety observers, and support staff.

2.3 Physical Security Assessment Methodologies

The security assessment is a comprehensive examination of the physical security posture of a plant that may serve as technical bases for evaluating an applicant's security program during the licensing phase, or to assess the effectiveness of an existing posture. The primary purpose of the assessment is to ensure that the physical protection system of a nuclear facility provides high assurance of protection against the design-basis threat (DBT), as proscribed in 10 CFR 73.55. This section summarizes the methodologies that were either directly used had an impact on the dynamic models developed in this research for assessment and optimization of physical security.

2.3.1 Vulnerability of Integrated Security Analysis (VISA) Tabletop methodology

Vulnerability of Integrated Security Analysis (VISA) Tabletop methodology was developed by Science Applications International Corporation (SAIC) for the U.S. NRC in 1976-1977 [17]. The VISA methodology can systematically evaluate effectiveness of nuclear security through the use of subject matter experts (SMEs). The methodology is a scenario-based approach based on subject matter expert opinion, documented values or a combination of both. The VISA process consists of four phases: 1) development of a general adversary scenario, 2) expansion of the scenario into logical steps (sensing and assessment opportunities), 3) analysis of the effectiveness for each individual step, and 4) determination of the overall scenario protection system effectiveness.

Phase 1 is a general attack strategy for theft or sabotage described by features such as numbers of adversaries, their specific capabilities, equipment, weapons, and intent. For nuclear power plant, the intent

is typically radiological sabotage and other features are derived from the design basis threat defined by the U.S. NRC in Title 10, Section 73.1(a), of Code of Federal Regulations [18].

Phase 2 expands the attack strategy from Phase 1 into logical steps, or events, based on site characteristics and credible scenarios that gives the adversary the best chance for success.

Phase 3 utilizes professional judgement by subject matter experts is used to determine each of the adjectival values (qualitative approach) or numerical values (quantitative approach) for the probability of sensing (P_S), probability of assessment (P_A), probability of interruption (P_I), and probability of neutralization (P_N). The values of P_S and P_A are step dependent while P_I is dependent on the adversary overall task/timeline versus the response force time. P_N is dependent on the response force size and capability to defeat the adversary assuming interruption occurs.

Phase 4 assigns percentage values for P_S, P_A, P_I and P_N using the qualitative approach of Phase 3. Take the lowest adjectival score (value) for each step and record it in the Step Score column (weakest link in the chain). Once each step scores are determined, use the highest Step Score value (strongest link in the chain) to determine the scenario Probability of Effectiveness ($P_{E)}$. The P_E step qualitatively summarizes the probability that the overall protection system of procedures, equipment, guards, and barriers will defeat the assumed adversary threat.

The VISA methodology has been popular traditionally for assessing the effectiveness of physical security. It is based on intuitive and logical approach, easier and faster to implement than other analytical methodologies, and requires minimal training and no specialized software tool. However, it has several limitations, the outcome is highly sensitive to human input and therefore the reliability of results can be questionable. One major limitation is that the number of scenarios generated are extremely limited, especially compared to the millions of scenarios that can be simulated by computer-based methodologies.

2.3.2 Design Evaluation and Process Outline (DEPO) methodology

The high-level steps of the DEPO methodology (ref) are shown in Figure 2 The DEPO methodology is a systematic approach comprising of three major steps, i.e., defining the Physical Protection System (PPS) requirements, designing a new, or characterize an existing PPS, and evaluating the PPS. The steps in determining the PPS requirements are as follows:

1. Characterizing the facility. This step involves investigating anything that may impact the performance of the PPS, which includes physical and environmental conditions, facility operations, facility policies and procedures, the existing regulatory requirements, safety considerations specific to each nuclear power plant, legal issues and corporate goals and objectives. Several examples to be considered in this step include whether the facility is surrounded by trees that may hinder offsite visibility, whether it is situated in a humid or arid area which may affect sensors' performance, if safety-critical equipment is located near the facility's perimeter, if it is legal to open fire to trespassers, or to install a surveillance system that monitors movements outside the facility's perimeters.
2. Defining the extent of threats to the facility. This step requires knowledge of the Design Basis Threat (DBT) set by the regulatory body. Each operator also needs to identify potential insider threats by assessing personnel's' job descriptions and access privileges.
3. Identifying and classifying the targets within the facility. This step involves listing the inventory of radioactive materials within the facility and categorizing them based on the existing regulations. It also identifies the list of components / equipment that may cause a significant damage to the reactor and causes a radiological release if they are sabotaged.
4. Researching the regulatory requirements and constraints. This step involves identifying the current regulations on physical protection of nuclear power plants, whether the protection requirements are explicitly prescribed in the regulation or whether the regulatory body promulgates a performance-based criteria instead.

The steps in designing a PPS system includes:

1. Designing the intrusion detection system, which includes the various sensors, cameras and lighting system. The sensor selection should be based on the facility characterization such as weather. Cameras and lighting should be selected and installed for an operator to quickly assess the situation when a sensor is tripped. Each sensor has different characteristics and flaws, therefore it may be beneficial to install multiple sensors with different operating principles for redundancies.
2. Designing the delay barriers. These barriers should be designed to slow down and delay the adversaries after they are detected by the sensors. It is meant to provide additional time for the response force to mobilize themselves and neutralize the adversaries before they finish their attack. These barriers may be in the form of passive barriers such as fences, reinforced doors, and walls, or active barriers that may be actuated upon demand such as smoke generators and sticky foam.
3. Configuring the response force requirements. The response force should have adequate manpower, skills and firepower to neutralize the threat as identified in the Threat Definition step. The team should also be stationed in a location that allows them to respond timely to adversary attacks before the attackers finish their attack plan.

The final step in the DEPO methodology is to analyze the performance of PPS design. This analysis is done through these following steps:

1. Evaluating the likelihood for the response force to interrupt adversaries before their attack plan is completed. The metric for this likelihood is termed as Probability of Interruption (P_I). This step requires the data on adversaries number, tools, capabilities, targets and their attack pathway. It includes simulations on adversaries attacks by taking into account the uncertainties on the intrusion detection system.
2. Evaluating the likelihood for the response force to neutralize the adversaries, given that they are able to interrupt the attack in time before the attack plan is completed. This analysis involves the comparison on the number and weapons of the response force versus the adversaries. The metric used in this analysis is termed as Probability of Neutralization (P_N).
3. Evaluating the overall effectiveness of PPS for a particular attack scenario. This analysis takes into account the attack scenario which includes among others the target sets, adversary's capabilities, and the attack pathway. This analysis uses a metric of PE, which is a product of P_I and P_N in a particular scenario. PE has a value from 0 to 1. A P_E of 0 indicates that the PPS always fail at protecting the target sets while a P_E of 1 means that the PPS is effective in protecting the targets.

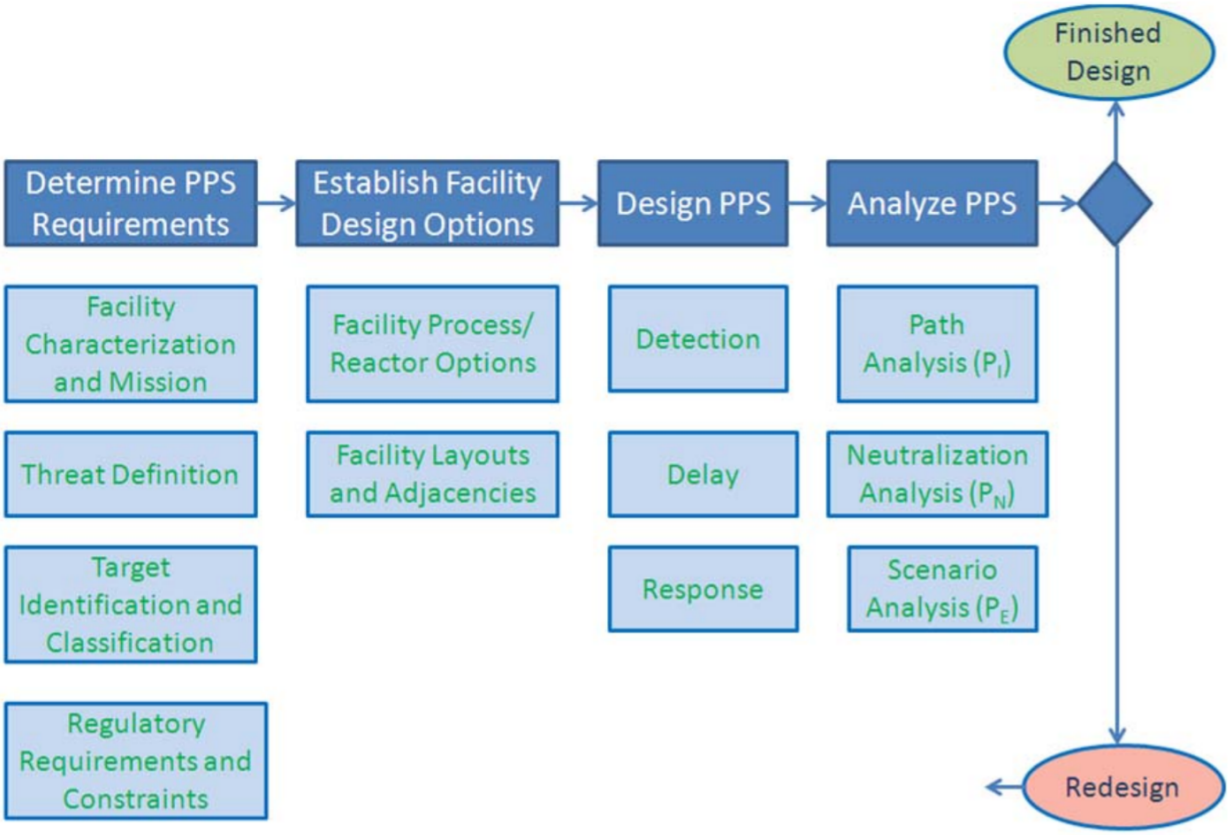


Figure 2. Design and Evaluation Process (DEPO) flowchart

2.3.3 Review of NUREG/CR-7145: Overall physical protection system effectiveness

The Nuclear Power Plant Security Assessment Guide NUREG/CR-7145 [14] published by the US NRC provides detailed guidance for the format and content of a security assessment at nuclear power plants. The guidance document is widely used to optimize physical security during the design phase, and in planning and executing changes and upgrades of physical protection systems at existing sites. The guidance document provides a detailed methodology for performing assessment of physical security system effectiveness.

Figure 3 shows the four-step security assessment process described in NUREG/CR-7145 [14].

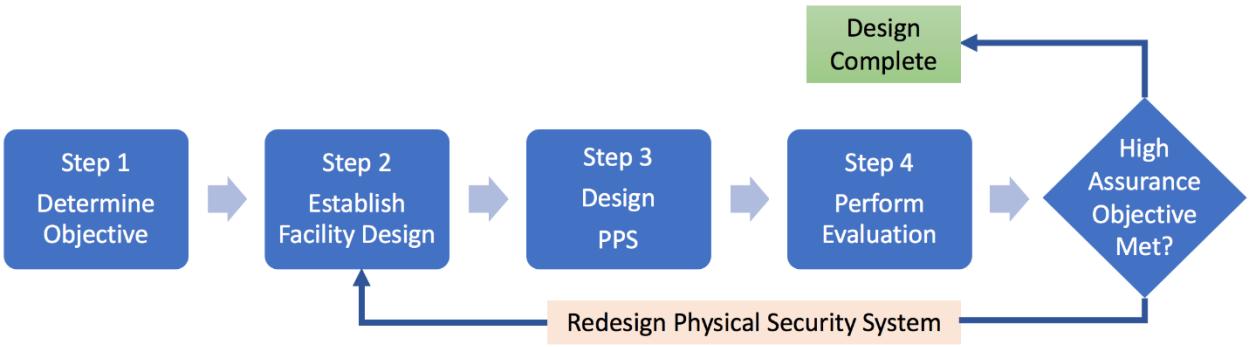


Figure 3. The security assessment process described in NUREG/CR-7145.

Determine Objective: The objective of physical security system is to protect the plant from radiological sabotage and prevent theft as defined by the NRC [13]. The US NRC provides a standard set of scenarios associated with the DBT that defines the characteristics of the adversary force such as force size, equipment, weapons, and tactics [13]. For a given standard DBT scenario there can be several overall scenarios based on variability in target sets, entry and exit points (for theft only), and other plant specific characteristics.

Establish Facility Design: Target set analysis is performed to establish the reactor facility design that must be protected by the physical security system. A radiological sabotage target set is the combination of equipment or operator actions which, if prevented from performing their intended safety function or prevented from being accomplished, would likely result in significant core damage [14].

Design Physical Protection System: The physical protection system at a nuclear power plant is a combination of equipment, people, and procedures with the combined aim of protecting the plant assets. This step characterizes the different elements of the PPS such as: detection, delay and response system, PIDAS, weapons, number of armed responders, number of patrolling officers, and strategic location of physical protection system.

Perform Evaluation: The physical security performance evaluation of step 4 is performed in three broad steps:

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

For a specific scenario, the adversary and responder timelines are developed. The adversary timeline provides a direct and quantifiable assessment of the different elements of the physical protection system for a given DBT. illustrates a typical adversary timeline for radiological sabotage.

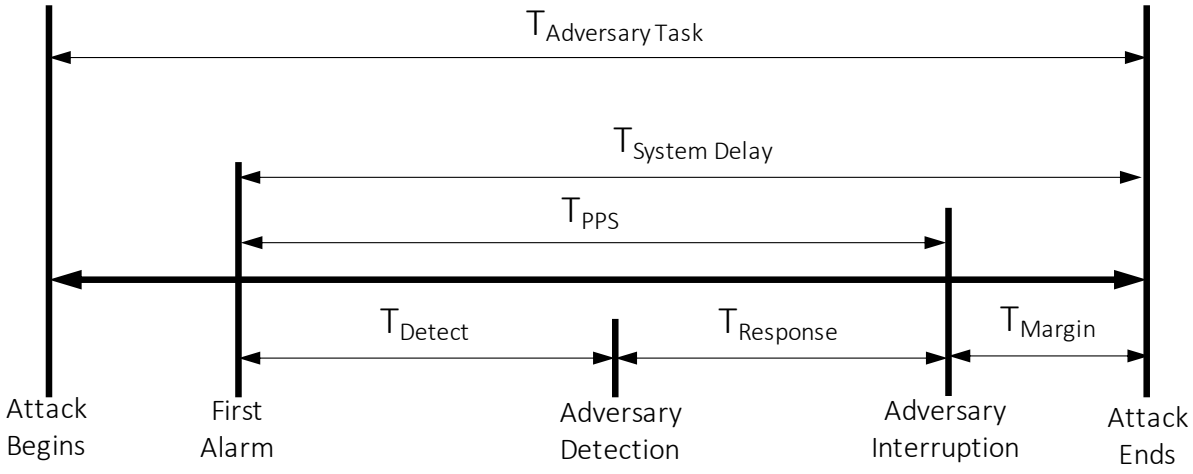


Figure 4. The timelines associated with an attack scenario.

Figure 4 shows an illustration of the timeline associated with an attack scenario. The $T_{Adversary\ Task}$ defines the time it takes the adversary to successfully accomplish the attack. This time can be estimated in a drill or mock scenario but is not known in a real attack scenario. The timeline truly begins at the instance of first alarm for the attack, from the first alarm to the successful detection of the adversary is the time to detection, T_{Detect}. Following the detection, the responders get in action in order to neutralize the attack, the timeline for responders to successfully interrupt or neutralize the attack is $T_{Response}$, which can reflect how effective the response team is in successful interruption or neutralization of the attack. The sum of T_{Detect} and $T_{Response}$ is T_{PPS}, which reflects the overall effectiveness of the physical protection system in timely neutralization of an attack.

NUREG/CR-7145 defines the overall effectiveness of physical security system as a probability:

$$P_E = P_I \times P_N$$

where P_E is the probability of overall effectiveness, P_I is the probability of interruption of the adversary, and P_N is the probability of neutralization of the adversary. From Figure 4 it is clear that the success of adversary interruption truly depends on the effectiveness and performance of the detection system, so P_I depends on probability of detection P_D. Detailed discussion on fundamentals of the probabilities and their estimation can be found in [6].

2.4 Force-on-Force Modeling

There are several levels and tools available for FoF modeling. The most basic level of modeling considered Table Top. There are several ways that a table top exercise can be conducted, but in its basic form, a group of Subject Matter Experts using a map or diagram of a facility simply postulate many attack scenarios and develop possible adversary attack paths and possible protective force responses. From these scenarios, the planers can determine what types of terrain and obstacles will have to be traversed and overcome. Once this has been determined, resources such as the Sandia developed Access Delay Technical Transfer Manual can be used to:

1. Determine what tools, ranging from mechanical to explosives, can be used to defeat the obstacle
2. For each tool, what will be the weight, and size
3. For each tool, what will be the time requirements to defeat the obstacle

And finally, for each tool, what will be the signature of the action, i.e., will it make a lot of noise over a longer period of time, will it have a bright light and heat signature, will it produce a loud explosion and shock wave that will be easily heard and felt by people inside the facility. Any of these signatures could affect the probability of detection and the probability of assessment.

Once the path and tool requirements have been determined, the planers can start to determine the number of adversaries required, the total adversary tool kit, including each adversary's individual part of the tool kit, and the basic adversary steps and corresponding rough timeline. Once this has been accomplished, more advanced computer modeling tools are used to refine and analyses the attack scenario.

Another version of the "Table Top" is often used in actual FoF exercises. When a situation is reached during the exercise that would be unsafe or cause damage to the facility, the exercise is usually put on hold at that stage, and the participants verbally step through the sequence. The expected outcome is determined by using accepted standards, such as the Sandia Access Delay Technical Manual, Computer modeling or performance testing that has been conducted and documented. Examples of this type of action are breaching of an obstacle. Whereas it is not possible, or wise, to actual detonate the explosives and destroy part of the plant's protective system, the adversaries would simulate many of the steps required to conduct the attack. The responding force would be verbally told what type of events they would be detecting; i.e., a loud noise, a bright flash, sensors or cameras going out. A hold is then placed on the exercise, while the adversary team is moved to the other side of the barrier. Once this has occurred, the exercise is resumed. This type of forced delays imposes a certain level of artificiality to the exercise. It is important that every step be taken to try and reduce this level of artificiality. The adversaries should be required to carry the equivalent weight of materials that would have been required and go through simulated actions to carry out the attack. Responding force personnel, should not be allowed to look around or observe actions during this time that would give them an advantage when the exercise resumes. Two phenomena that are difficult or impossible to account for during these delays are (1) during these forced delays, people are able to recover from physical exercise, and the human brain will remain active, reviewing the actions that have occurred, and (2) formulating possible scenarios that might be occurring, and formulating appropriate responses to these actions. The above two phenomena underline the extent to which FoF exercise can accurately simulate a real-life attack scenario.

More advanced tools are now being used by industry which use path analysis algorithms, human response models and Monte-Carlo simulation runs to evaluate attack scenarios and defense strategies. The main tools used by industry are AVERT by ARES Security [9] and Simajin by RhinoCorps [10]. These tools allow utilities to model their facility in a 3D environment with detection and protection equipment such as the PIDAS, BRE's, vehicles, etc. The modeler can also input time requirements for movement, delays, probability hit probability kill (PHPK), cover protection, firearms, equipment, etc. After a model is complete it has several uses, such as evaluating likely attack routes; evaluating current defense measures; or testing specific scenarios. Results from these tools can give a statistical analysis or the probability of success for attacks.

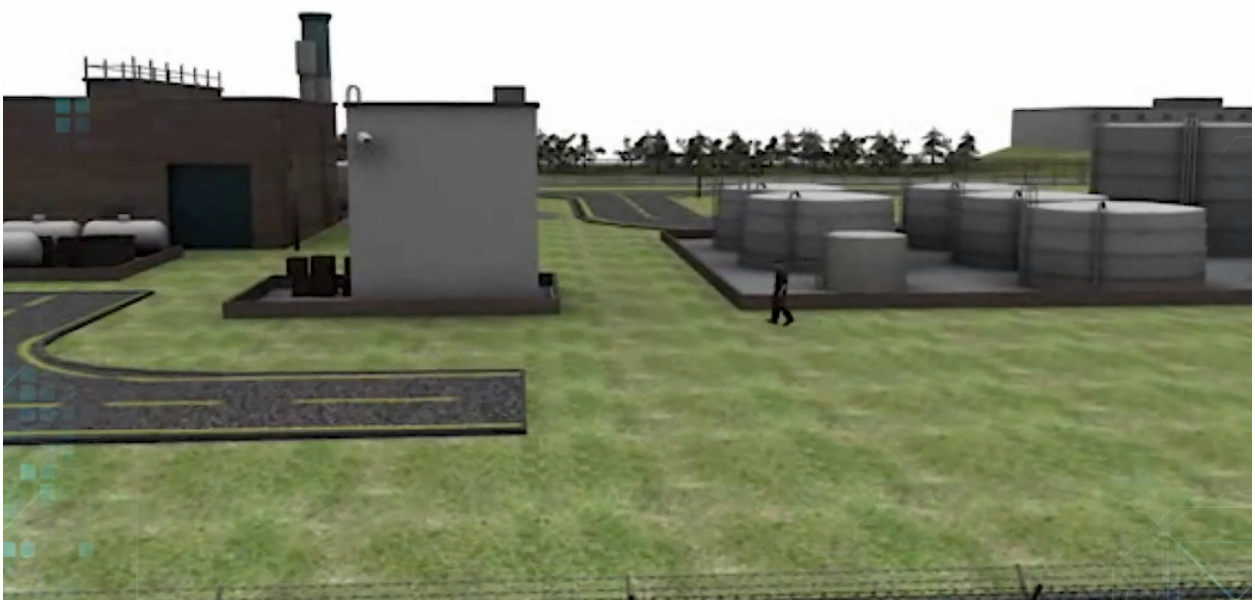


Figure 5. 3D model of a nuclear power plant in AVERT software

These modeling tools provide accurate modeling of scenarios and probable outcomes but focus on the attack itself. They do not include or vary the probability of attack, alert levels, environmental conditions, current plant conditions, operator actions during or after the attack, etc.

3. PHYSICAL SECURITY OPTIMIZATION

In order to justify optimization changes in a physical security posture, according to section (p) of NRC's 10 CFR 50.54 [19] it must be shown that the changes do not reduce the effectiveness. To act as a standard, we outline a process for evaluating potential strategy or equipment changes and determining the staff reduction made possible by using those changes while showing the maintained effectiveness. Much of this process could be automated with software once the first Base Case Evaluation is completed.

3.1 Base Case Evaluation

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

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

the adversary force beyond the DBT, followed by rerunning the FOF model and observing the change in effectiveness. While the DID should not drastically reduce the effectiveness, the number of failed evaluation cases should significantly increase. For example, in 5,000 simulations, if the base case effectiveness is 98%, only 100 evaluation cases are available, but, with a DID model of 91% effectiveness, 450 cases would be generated from the 5,000 simulations. The key is to capture the failure cases and the avenue of those failures from the simulation. If a certain DID model causes the same few avenues for failure as the original base case, other DID models need to be modeled or additional attack scenarios should be included to add additional failure paths. The evaluations corresponding to failure cases will be used to evaluate the modified strategies and can clearly identify improvements or defense reductions where only using the original base case tests would show little to no change.

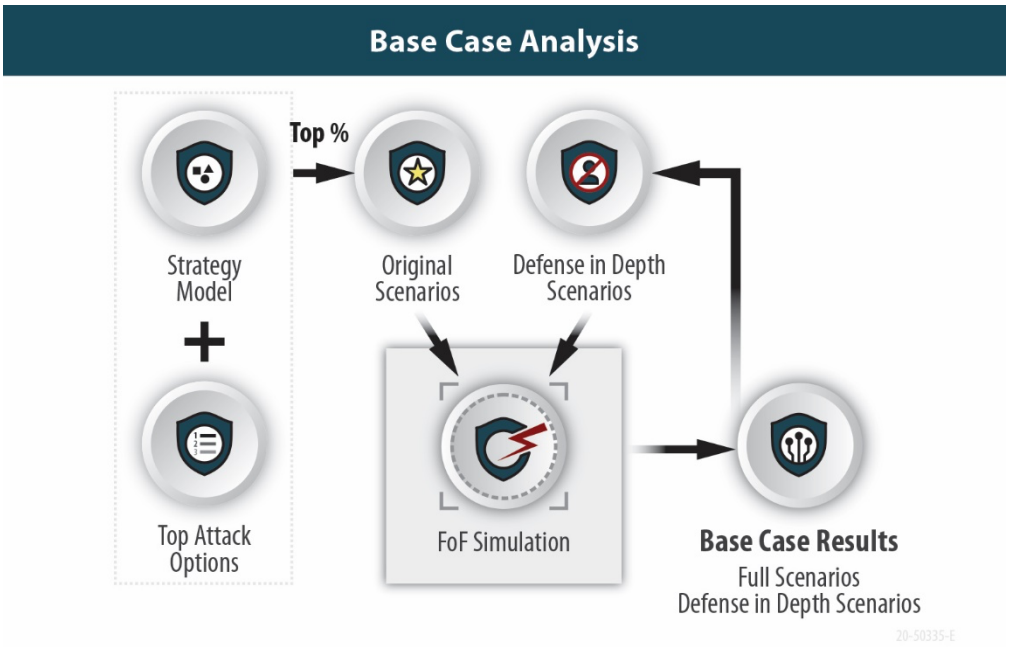


Figure 6. Flow for creating base case comparison results.

Many facilities currently have a previously evaluated defensive strategy model, and these can be used as a starting point to develop the comparison base cases. In summary, the process for developing the base case results are the following steps, as shown in Figure 6:

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

3.2 Potential Strategy Evaluation

Each facility can have different options they consider for optimizing their defensive posture. Some options can be evaluated in a research setting for a variety of facilities meeting defined conditions. Others could be site specific, and a potential evaluation should be done to determine the probable and best improvement options before the full in-depth modeling process is done and evaluated, as described in Section 3.1.

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

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

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

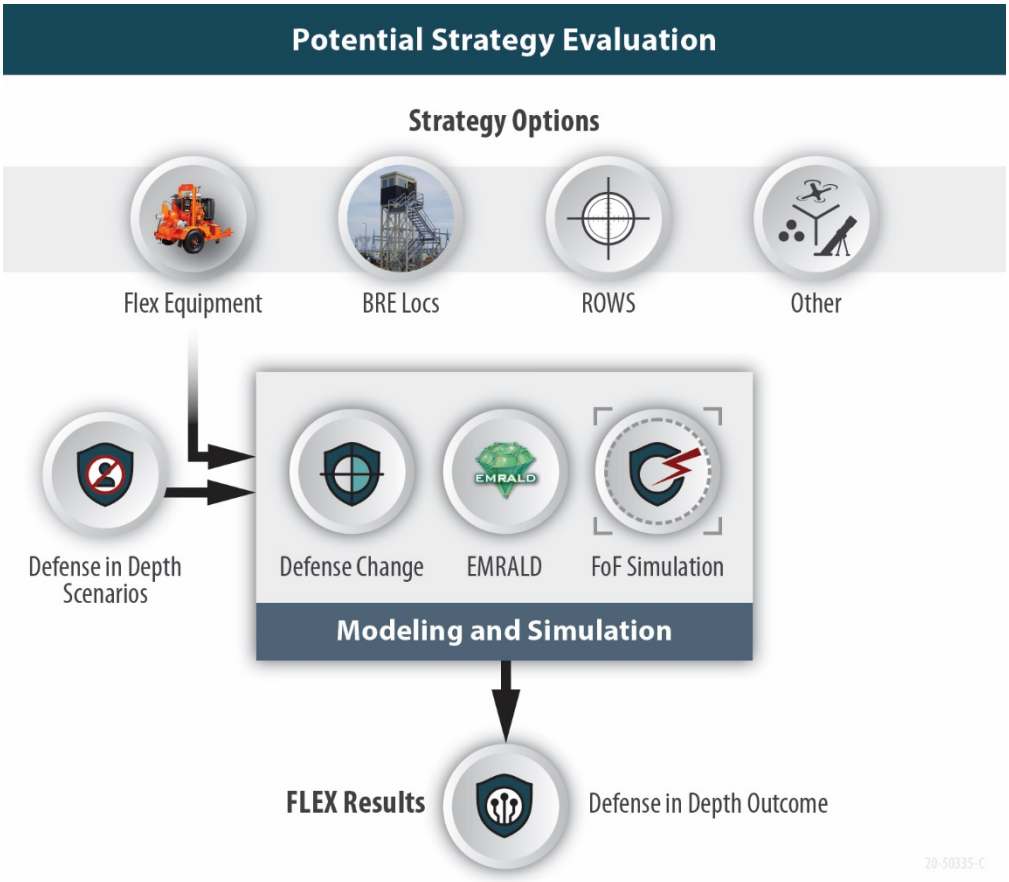


Figure 7. Flow for option evaluation.

In summary, the following steps are used to evaluate a potential strategy protection option, shown in Figure 7:

1. Determine likely improvement methods for strategy change
2. Build a model of those changes using an appropriate tool or tool combination

3. Apply the DID scenarios to the new model/s and run the simulations
4. Compare the results to the original DID results.

3.3 Staff Reduction Evaluation

Once likely improvement methods have been identified and modeled, the process for determining a staffing reduction can begin. This process will ensure that even after a potential staff reduction, an equivalent protective strategy is maintained, at least at its current level. The four main steps to this process are outlined in Figure 8 and described in the steps below. Before the process begins, a copy of the original and DID base case simulation scenarios and results is made. This is an iterative process and stops once the criteria has been met.

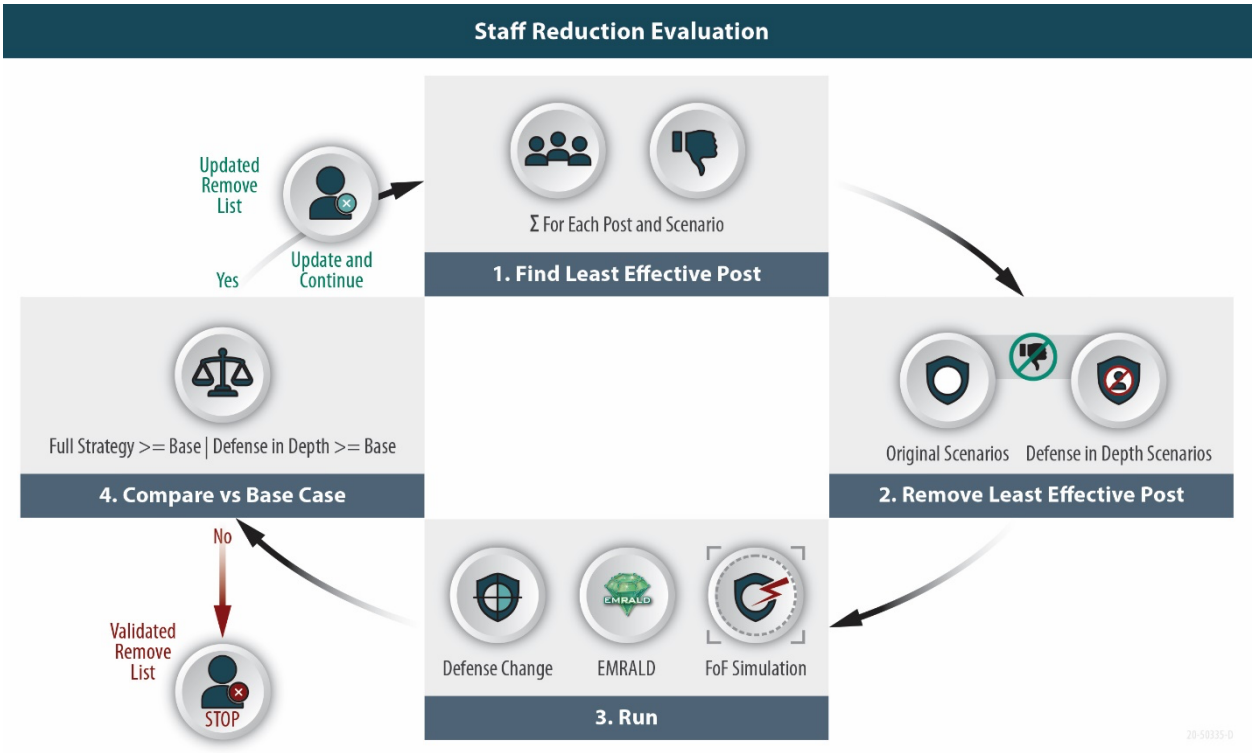


Figure 8. Process to evaluate staff reduction for a strategy change.

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

Once the process has stopped, the posts in the "validated remove list" contains the posts that can be eliminated if the new strategy is implemented.

This process takes a conservative iterative approach and does not account for the possibility of correlated posts where a combination of possibly more effective guards could be less impactful than iteratively removing the worst, one at a time.

4. APPLICATIONS FOR POTENTIAL STRATEGY EVALUATION

4.1 FoF-FLEX Integration

The current regulation on the physical protection of NPPs promulgates the requirements to prevent radiation exposure to the public through deliberate actions [4]. As such, the physical protection system is designed to prevent sabotage actions on specific combinations of targets, termed as target sets, that can cause the plant to undergo a catastrophic failure and release radioactive material into the environment. The protection measures are considered as failed when a target set is sabotaged. This approach provides a clear and simplified acceptance criterion to the protection system design objective. However, it is understood that such a criterion contains a conservative assumption, which undermines the fact that there is a period of time from the moment a target set is damaged to the time when the plant undergoes a catastrophic failure.

The aforementioned time-margin can be utilized to perform mitigation actions in order to prevent plant damage. This section describes how FLEX mitigation strategies can be leveraged for this purpose. These strategies rely on the use of FLEX portable equipment to provide backup power and/or heat removal from the reactor. It is well known that the preparation and operation of these portable equipment are done manually and, therefore, execution times may vary significantly for different plants and scenarios [20]. In order to capture these timeline variations and assess the feasibility of these FLEX strategies, a dynamic framework of FOF and FLEX modeling approach is pursued.

The overview of the dynamic framework of FOF and FLEX model integration is illustrated in Figure 9. The integration starts with the FOF simulation being conducted using a commercial FOF software. The FOF simulation provides the attack timeline data as well as the targets' conditions at the end of the attack. This data is read by EMRALD to determine the proper timing to start the preparation of the FLEX portable equipment. This stage may include communication and coordination with field personnel, equipment mobilization, staging, and connection. The mobilization and staging phase may be skipped if the FLEX equipment is pre-staged. Dynamic uncertainties of the FLEX preparation, as modeled in EMRALD, create a statistical distribution of the timeline of FLEX equipment being operational. At the end of the attack scenario, EMRALD fetches the list of targets and their conditions from the FOF simulation output. The EMRALD model uses this data to decide the applicable mitigation strategy as needed. If the attack is not successful at all, the plant may continue its normal operation. Meanwhile, if several components or equipment are sabotaged, but the plant still retains its design basis safety functions as maintained by intact redundant or standby components, the mitigation is accomplished using the design basis systems. Lastly, mitigation strategies using FLEX equipment are conducted when the safety functions of the design basis systems are lost due to the sabotage attack. The execution of this FLEX strategy depends on which safety functions are lost after the attack.

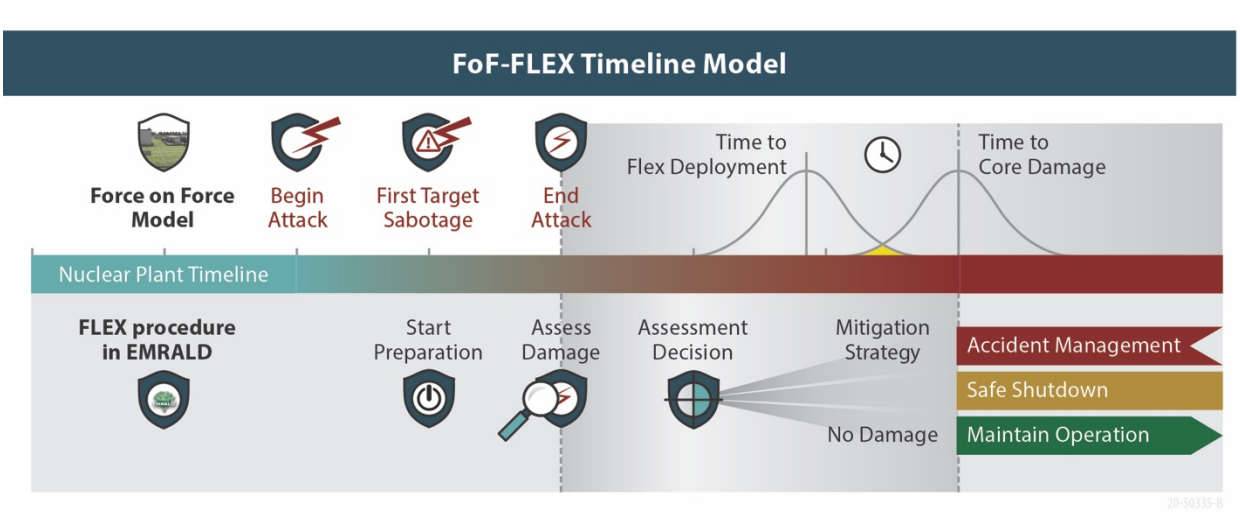


Figure 9. FOF-FLEX integration framework.

4.1.1 FLEX Equipment

FLEX equipment consist of mobile equipment that can be relocated to various locations within the nuclear power plant complex in order to provide electrical power, water pumping and/or other functions required to support a safe shutdown of the plant when the design basis equipment are not available. Several pictures of FLEX equipment are shown in Figure 10. A more detailed list of FLEX equipment and their functions for Boiling Water Reactors (BWRs) and Pressurized Water Reactors (PWRs) are provided in reference [21].

Figure 10. FLEX mobile equipment

A case study is described in this section to demonstrate the applicability of the FOF-FLEX integration model. A hypothetical attack scenario to a hypothetical PWR plant was developed in this case study. This case study does not use any plant proprietary data or information. In the attack scenario, a group of adversaries attempts to cause a radiological release by sabotaging the plant's power supply and its ultimate heat sink capabilities. The attack follows the event progression highlighted in red in Figure 11, which is adopted from a station blackout event tree for a PWR plant [22].

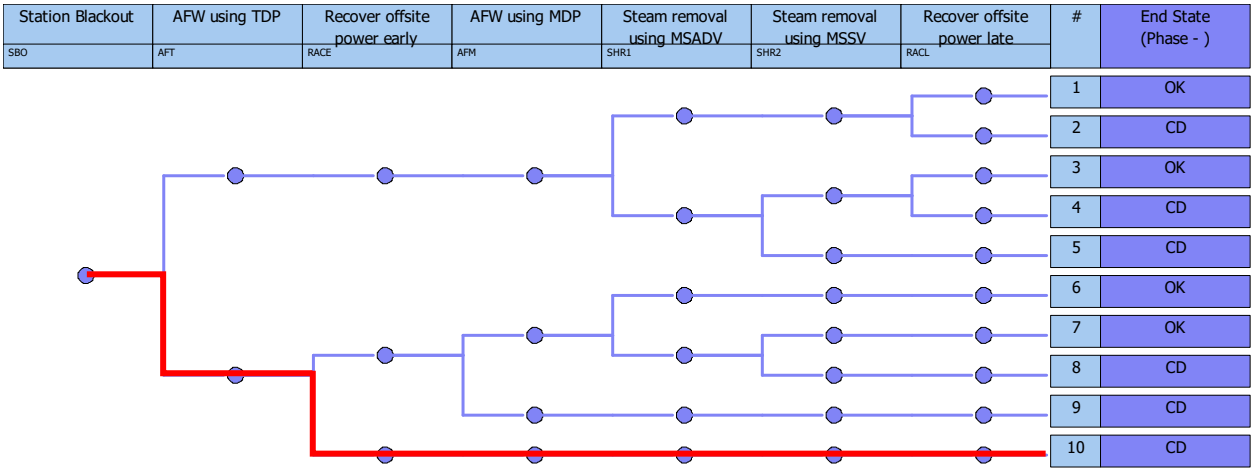


Figure 11. Sabotage scenario to inflict core damage.

Targets and the attack pathway to inflict the aforementioned core damage progression are shown in Figure 12. An adversary sets explosives at an unmonitored grid tower outside of the nuclear plant complex to cause a loss-of-offsite-power (LOOP) event. Meanwhile, a group of armed adversaries enters the complex to sabotage the emergency diesel generators (EDGs) to cause a station blackout (SBO) event and damage the turbine driven pumps (TDPs) to disable the plant's passive heat removal capability. The plant has its physical protection program in place, consisting of the intrusion detection system (IDS), delay barriers, and both the stationary and mobile response force. These protection elements are not shown in Figure 12 to provide a visual clarity on the attack path and target locations. If all of these targets are sabotaged, the nuclear plant will experience the core damage (CD) state within an hour [22].

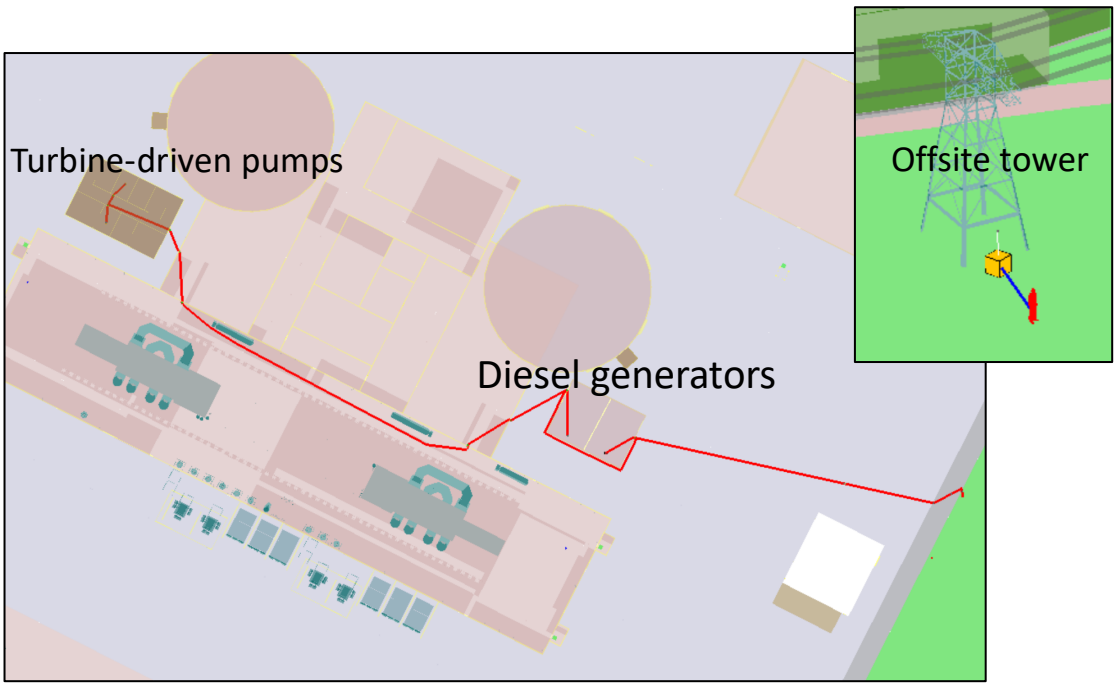


Figure 12. Attack targets and path in the force-on-force model.

A list of all possible outcomes from the attack scenario is shown in Table 1. If adversaries fail to sabotage any system in the target set, as indicated in the first outcome, the plant may continue its normal operation. Meanwhile, if the plant loses several of its safety functions without the initiation of safety-related events, as listed in Outcomes 2 through 4, the plant stops its operation in order to repair the damaged safety systems. If the initiating safety event occurs, it is mitigated with the design basis safety systems if they are available, as shown in Outcomes 5 and 6. Otherwise, the FLEX equipment are used to substitute the safety functions of the damaged design basis systems, as explained in Outcomes 7 and 8. FLEX Strategy A entails the use of FLEX equipment to provide the emergency power needed for the prolonged heat removal using TDPs. Meanwhile, FLEX Strategy B consists of utilizing the FLEX diesel generator to provide power and FLEX pumps to supply feedwater to the plant's secondary side. The time period to perform these FLEX strategies are taken from a reference study [22].

Table 1. Possible attack outcomes.

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

4.1.2 Sequential FLEX Implementation

The procedure to implement a FLEX strategy in this case study is shown in Table 2. Steps in this procedure were categorized into preparation and execution stages of the FLEX strategy. Preparatory actions are done prior to executing the FLEX mitigation strategy, as illustrated in the "Start FLEX Preparation" step in Figure 9. After the FOF simulation is completed, an assessment is done to determine the plant condition. Based on this assessment, the appropriate FLEX strategy is performed, following the execution actions in Table 2.

Table 2. FLEX Procedure.

Number	Steps	Notes
1	Get keys and open doors	Preparation
2	Assess condition of plant system & equipment	Execution
3	Contact Strategic Alliance for FLEX Emergency Response (SAFER) control center to inform the extended-loss-of-ac-power event	Execution
4	Connect FLEX steam generator makeup pumps' hose	Preparation
5	Establish configuration to support FLEX 480V ac installation	Execution
6	Connect FLEX cables to 480V MCCs	Preparation
7	Open all breakers on MCCs	Execution
8	Connect FLEX RCS Makeup pump hoses	Preparation
9	Inform Security of security area access breaches	Execution
10	Put a FLEX diesel in service	Preparation
11	Restore partial lighting and receptacle power	Execution
12	Turn on supply breaker in FLEX diesel generator enclosure	Preparation
13	Evaluate potential usages for the portable equipment being delivered from RRC	Execution
14	Ensure support equipment are staged	Preparation
15	Establish communication	Execution

The dynamic framework in Figure 9 is modeled in EMRALD, as shown in Figure 13. The process begins in the "Start" state, where variables in the model are initialized to their default values. Then, the model proceeds to the "Read_Avert" state, in which it runs the preconfigured FOF model built into the commercial AVERT platform and fetches the results from that simulation. The model proceeds to the "Plant_Continue_Operation" state if there is no damage to any components within the target set. Meanwhile, at the time when the first component is sabotaged, the model continues to the "FLEX_Preparation" state.

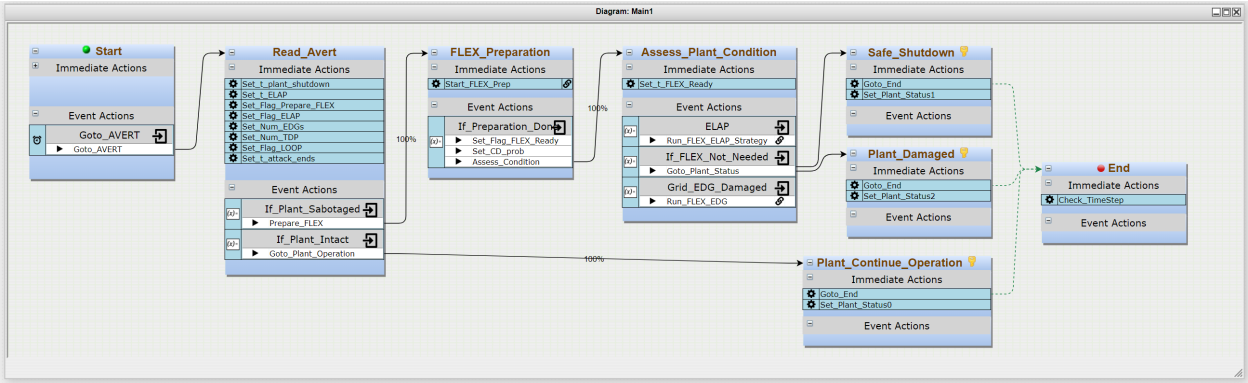


Figure 13. Main diagram of EMRALD model.

The immediate action named "Start_FLEX_Prep" within the "FLEX_Preparation" state transfers the simulation to the "Keys_and_doors" state in an EMRALD subdiagram shown in Figure 14. This subdiagram details the preparation of FLEX equipment, as shown in Table 2, which includes aligning the makeup pumps, starting the FLEX diesel generators (DGs) and connecting the electrical cables. Uncertainties on the completion time of actions shown in this subdiagram were modeled following a normal distribution. Upon starting the FLEX DGs, there is a statistical probability for the DGs to fail-t-start and to fail to continuously run. If any of those failures happen, the simulation transitions to the "FLEX_DG_Status" state in which a repair action is performed. Uncertainties in the timing to repair DGs and the success probability are modeled in EMRALD. After all the preparation actions are completed, the event action "Set_Flag_FLEX_Ready" triggers the "If_Preparation_Done" event in the main diagram shown in Figure 13.

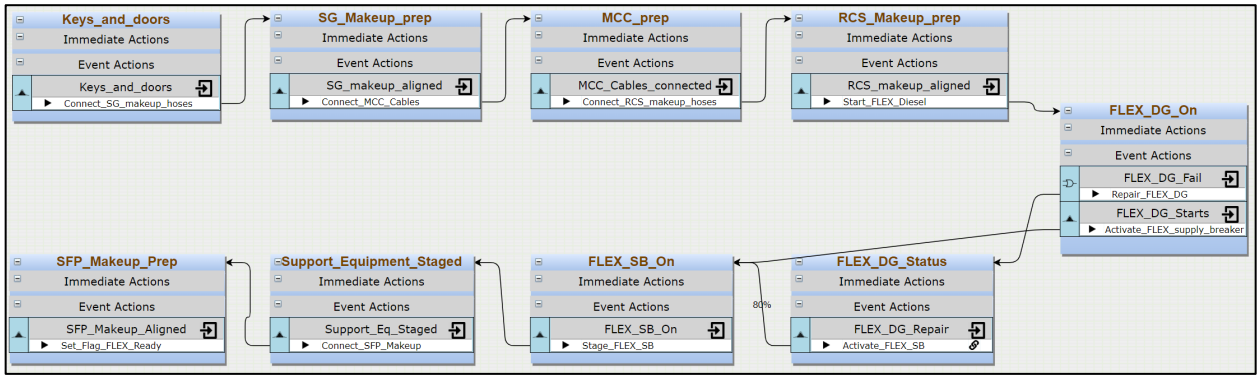


Figure 14. Sequential preparation of FLEX equipment.

The component failure diagram for FLEX DGs are shown in Figure 15. Initially, the component is in the "FLEX_DG_Standby" state while it is not in use. When the EMRALD simulation enters the "FLEX_DG_On" state in Figure 14, it triggers the "FLEX_DG_Demand" in Figure 15. The component's failure to start up on demand is represented by the arrow leading to the "FLEX_DG_Fail" state with a probability of 1E-2. The "FLEX_DG_Active" state is active if the component starts successfully. The

"FLEX_DG_FR" event contains the component failure rate and the required mission time data, which is set as 24 hours in this case study. Any fail-to-run event within this mission time triggers the "FLEX_DG_Fail" state. If both FLEX DGs are in this state, the "FLEX_DG_Fail" event in Figure 14 is activated. This event leads to an attempt to repair the FLEX DGs with a success probability of 0.8. This repair will cause the simulation to switch from the "FLEX_DG_Fail" state to the "FLEX_DG_Active" state.

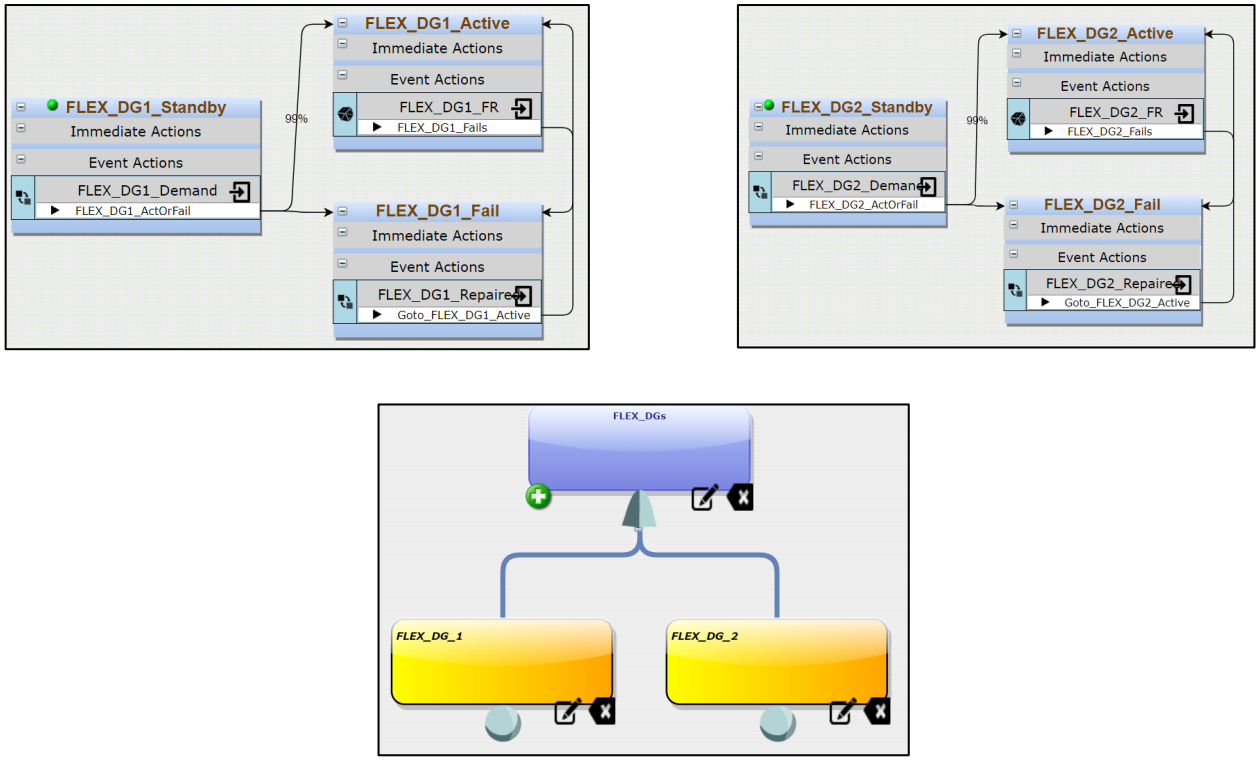


Figure 15. FLEX DG failure model.

The diagram for the failure of FLEX auxiliary feedwater (AFW) pumps is shown in Figure 16. This model is similar to the failure model for the FLEX DGs. However, repair actions are not included for FLEX AFW pumps for simplification. Furthermore, the failure rate for FLEX AFW pumps are also adjusted accordingly for pumps.

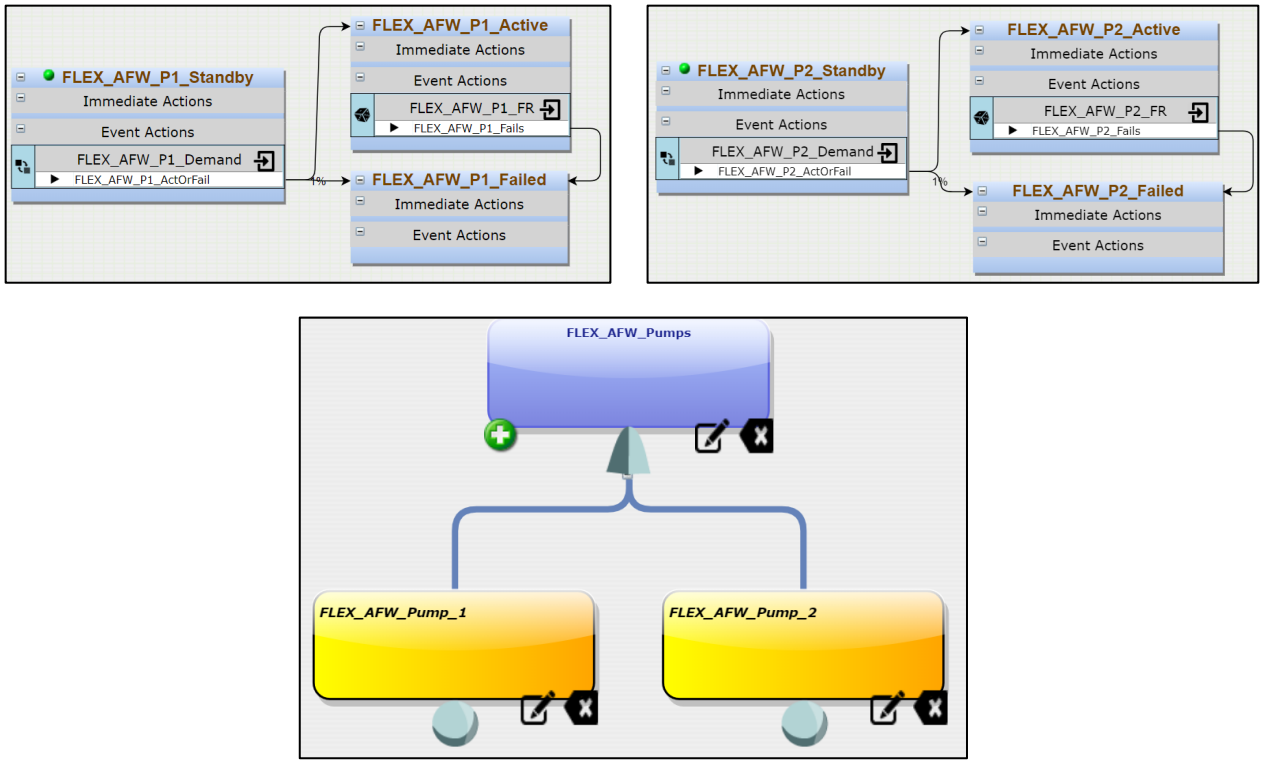


Figure 16. FLEX pump failure model.

Figure 17 shows the EMRALD model of the execution of FLEX strategy. The starting "Check_FLEX" state is actuated from the "Assess_Plant_Condition" state in Figure 13. It is followed with actions to execute the FLEX strategy, which include direct current (dc) load shedding, opening the electrical breakers, aligning the steam generator (SG) pumps, performing the pump transfer switch, and maintaining the FLEX strategy for 24 hours. The time distribution on each action is modeled in each event. The end "FLEX_ELAP_Strategy" state checks if the FLEX components run successfully for the entire mission time of 24 hours and ends the simulation with the "Safe_Shutdown" state if they do.

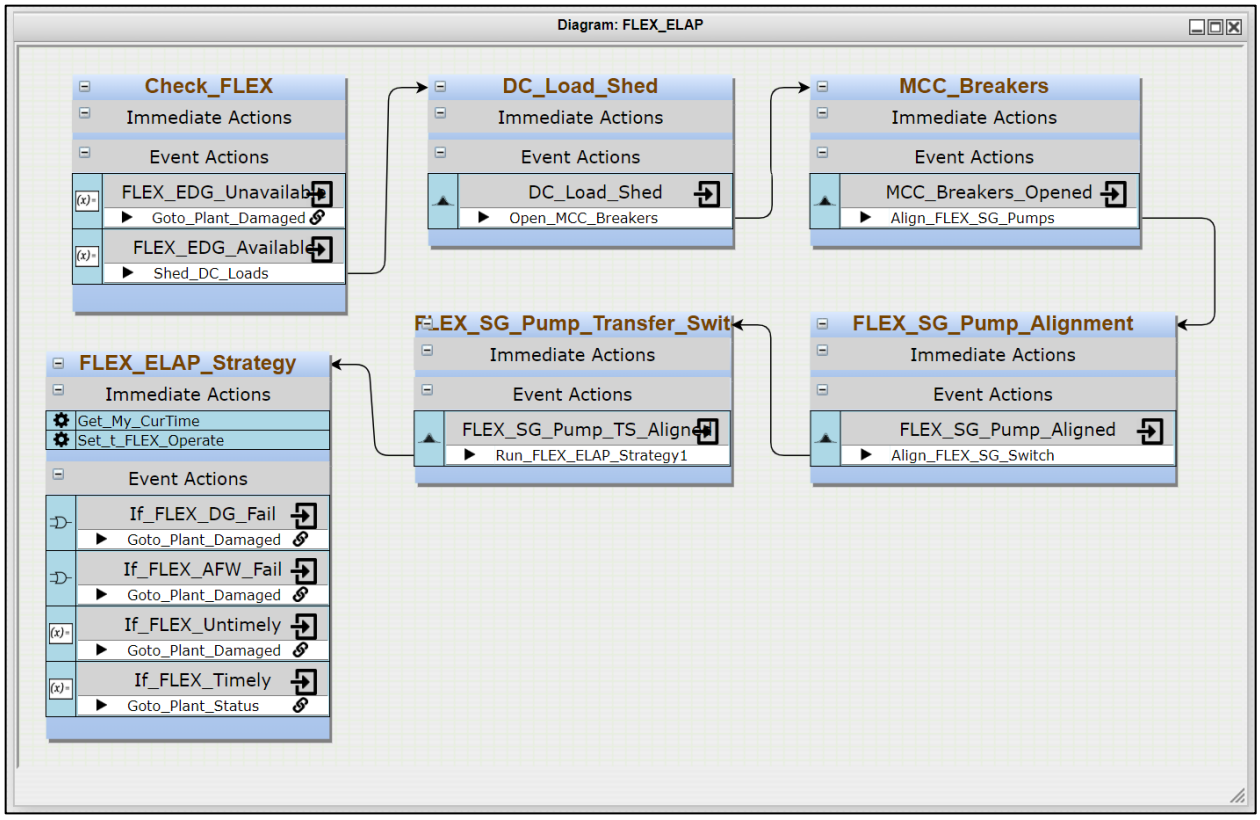


Figure 17. Sequential execution of FLEX strategy.

4.1.3 Parallel FLEX Implementation

The previous section presented the EMRALD model when actions in the FLEX strategy are performed sequentially. However, several of the FLEX actions, such as preparations of pumps and electrical components, can be done in parallel. Parallel implementation of FLEX actions may reduce the equipment preparation time before the reactor is damaged, potentially increasing the success likelihood of the FLEX strategy. In order to analyze the benefits of a parallel FLEX implementation, we modeled the FLEX preparation actions in EMRALD, as shown in Figure 18. In this subdiagram, the preparation steps for the electrical system are done simultaneously with the steps to prepare pump connections. This parallel action is made possible by the "Connect_MCC_Cables" action in the "SG_Makeup_Prep" state. The sequence from the "MCC_prep" state to the "FLEX_SB_On" state is simulated in parallel with the sequence of the "SG_Makeup_prep" state to the "SFP_Makeup_Prep" state. The simulation control is returned to the main diagram in Figure 13 upon reaching the "Support_Equipment_Staged" state.

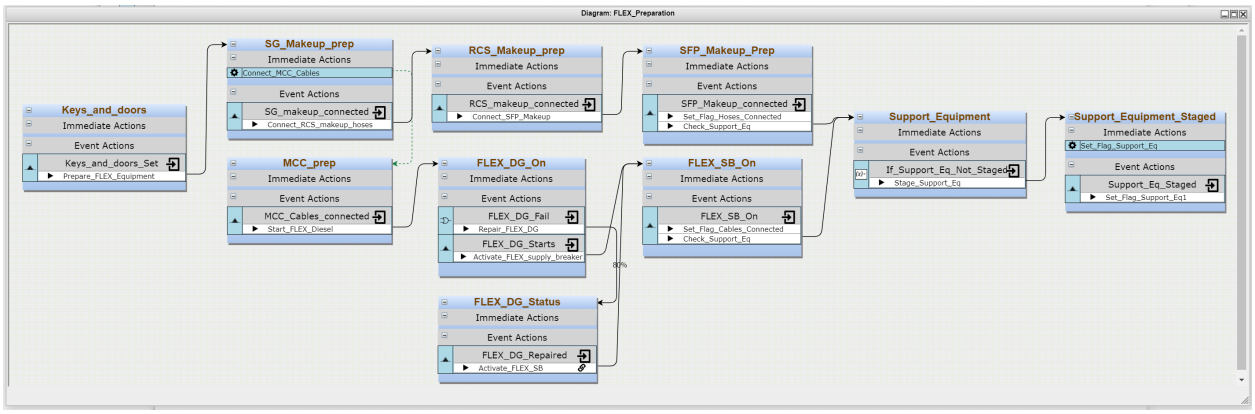


Figure 18. Parallel preparation of FLEX equipment.

The execution of FLEX strategy to provide alternating current (ac) power in case EDGs are sabotaged is shown in Figure 19. The process starts with a conditional check to ensure that the FLEX DGs are available before performing the dc load shedding and opening the electrical breakers. The "FLEX_EDG_Running" state models the FLEX DG probabilistic fail-to-start event and the failure to continuously run event as previously described. The simulation activates the "Plant_Damage" state when FLEX strategy is performed too late or when there are random failures of FLEX equipment within the required mission time.

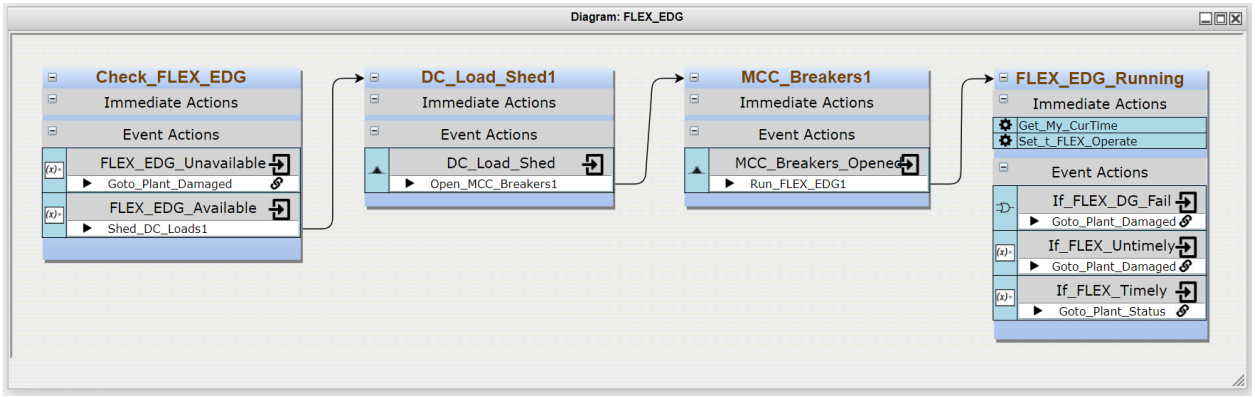


Figure 19. FLEX EDG strategy.

In the event where all components within the target set are sabotaged, the FLEX extended loss-of-ac-power (ELAP) strategy is executed following Figure 20. The subdiagram starts with conditional events to check whether FLEX DGs are still running prior to shedding the dc load and opening the breakers. These actions are done simultaneously with the alignment of the FLEX SG makeup pumps. Upon the completion of these two states, the "When_FLEX_ELAP_Ready" event is activated. Probabilistic events of random failures of FLEX equipment are modeled in the "If_FLEX_DG_Fail" and "If_FLEX_AFW_Fail" events.

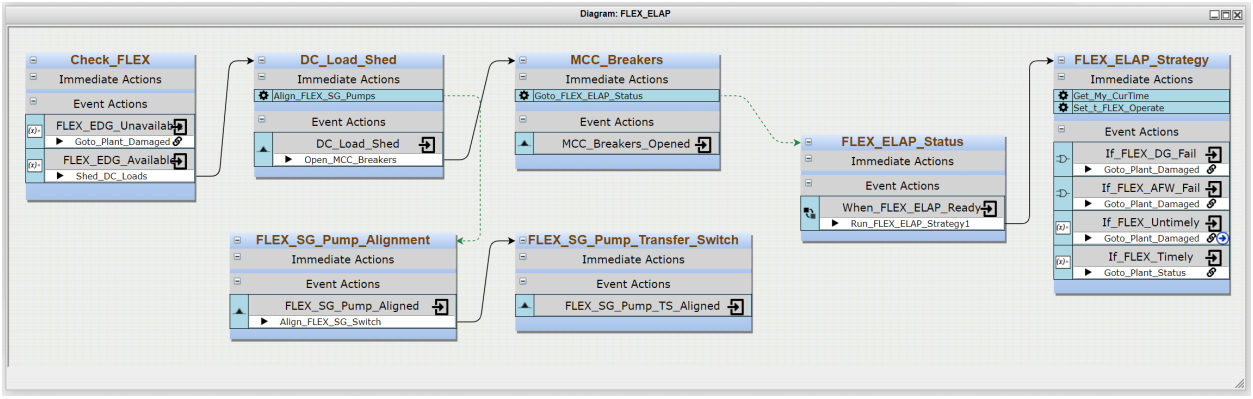
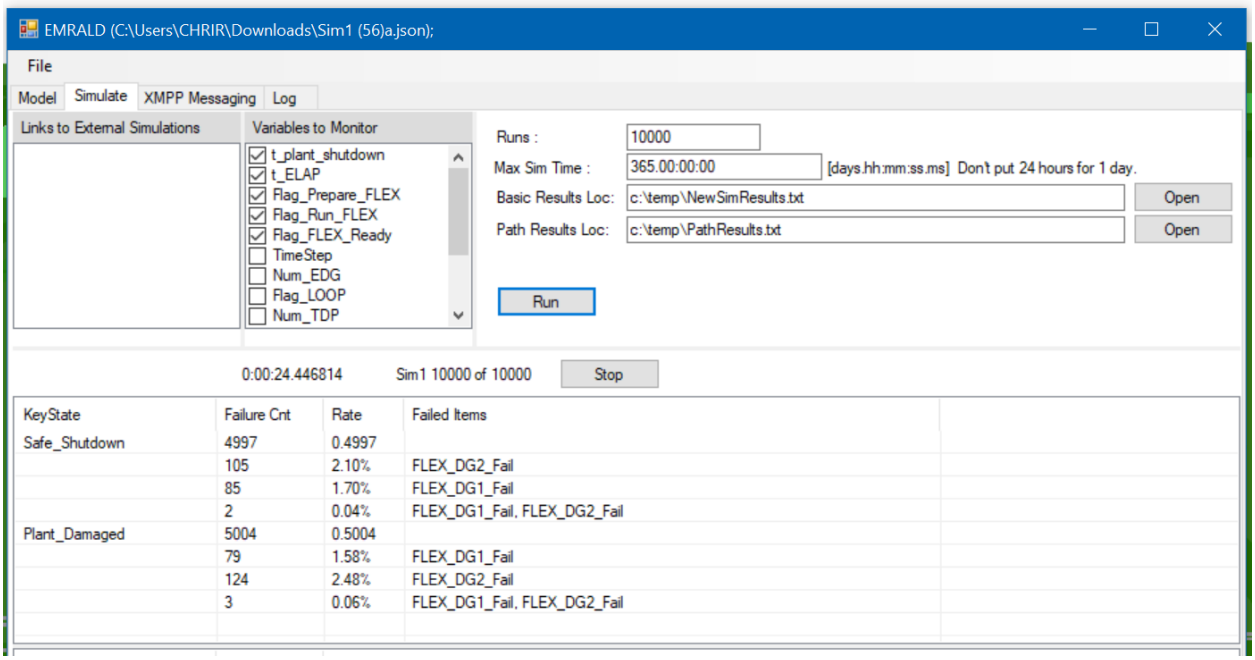


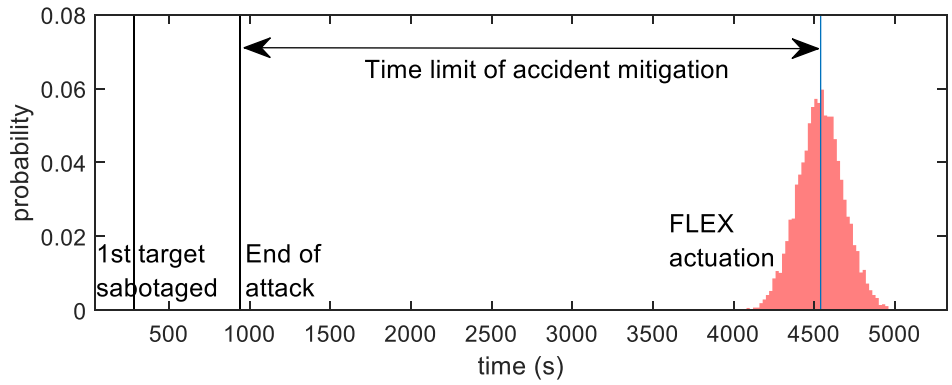
Figure 20. FLEX ELAP strategy.

4.1.4 Results and Discussion

The EMRALD model explained in the previous section was saved as a text input file and was solved using the EMRALD solver. The solver is a separate standalone software that runs the input file with a Monte Carlo sampling technique and tallies the number of key states encountered by each simulation. The solver window for the sequential FLEX actions is shown in Figure 21(a). It ran the model using ten thousand random instances and showed that it has a nearly 50% probability of reaching a safe shutdown state. Further details are shown in the form of a timeline in Figure 21(b). It shows the distribution of the FLEX actuation timing. Without the FLEX strategy, this particular FOF scenario would have resulted in a radiological release event. However, by using the FLEX mitigation strategy, there is about a 50% probability that such an event could be prevented in a timely manner. This result shows that FLEX can be utilized to mitigate the adverse effect of sabotage-induced events.



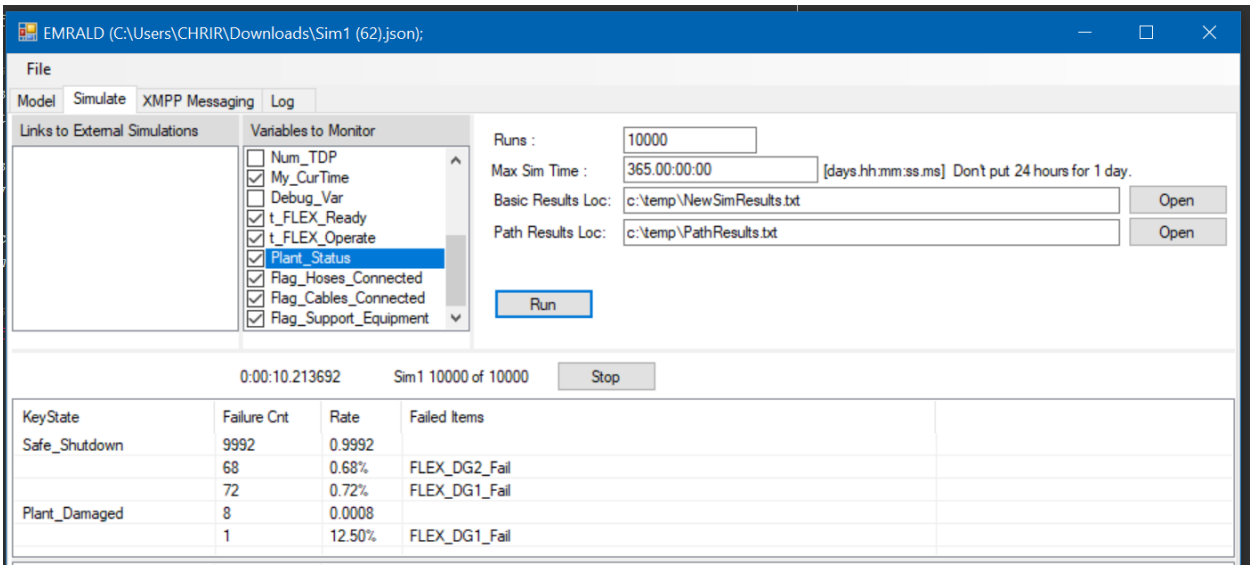
(a) EMRALD Results



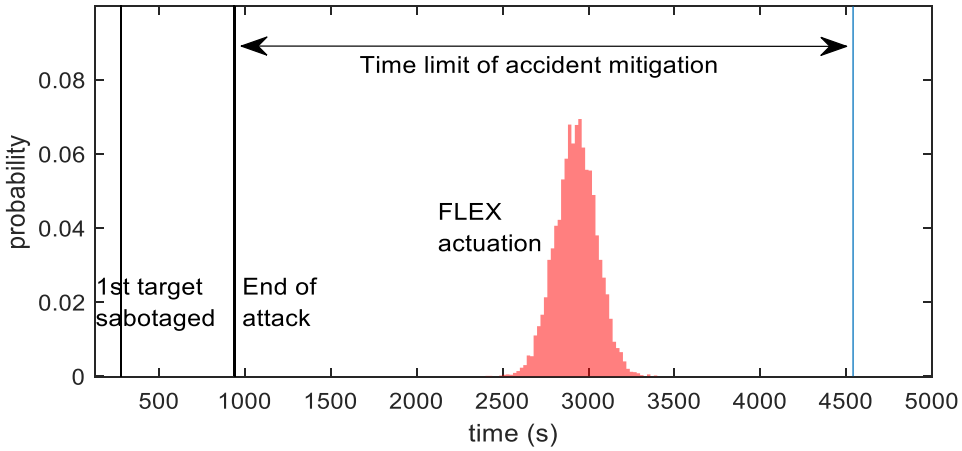
(b) Timeline Evaluation

Figure 21. Results of sequential FLEX actions.

Although the results from the sequential FLEX model show the benefit of the FLEX strategy in physical security, it can be improved further by reducing the time required to prepare the FLEX equipment. For that reason, we investigated the EMRALD model on the parallel FLEX actions as well. Results from this model are shown in Figure 22. The figure indicates that a parallel execution of the FLEX mitigation actions could shorten the actuation timing such that the success probability of the FLEX strategy was increased considerably. The small chance of plant damage of 8E-4 might be caused by random failures of the FLEX equipment.



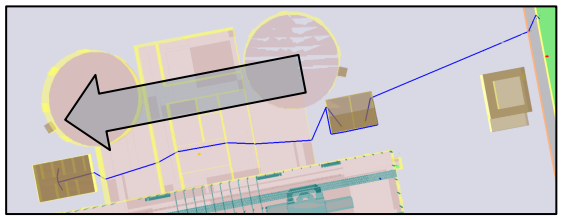
(a) EMRALD Results



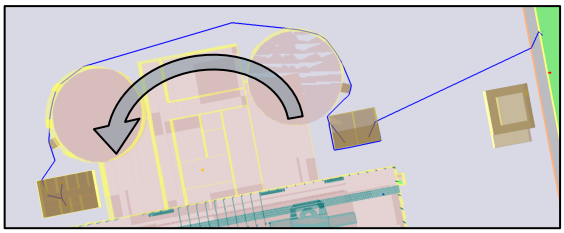
(b) Timeline Evaluation

Figure 22. Results of the parallel FLEX actions model.

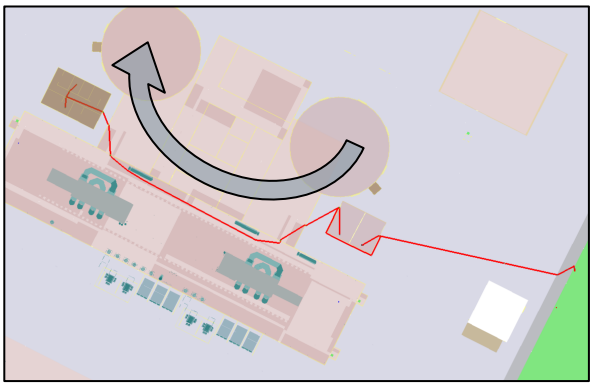
The results shown in Figure 21 and Figure 22 were obtained from a single FOF simulation such that there are discrete time points when the first target was sabotaged, when the attack ended, and the time limit to actuate the FLEX strategy. In practice, there are uncertainties within the FOF analysis that originate from the adversary exact attack path, the IDS, the adversary and response force's timing, and the adversary neutralization event. In order to capture these uncertainties, the FOF simulation was repeated multiple times. Three adversary attack paths of the shortest-distance and two detour paths were evaluated, as shown in Figure 23. For each of these paths, 100 Monte Carlo runs were simulated, resulting in a total of 300 simulations.



(a) Attack Path 1



(b) Attack Path 2



(c) Attack Path 3

Figure 23. Attack paths for the FOF scenario.

The outcome of the 300 FOF simulations are tabulated in the "Probability" column of Table 3. As given in the Table, there were several outcomes with zero probability. Outcome 1 through 4 were not observed due to the facts that the electric tower is located offsite and, therefore, it is not protected. Meanwhile, Outcome 6 did not occur because the TDPs are located further inside the plant complex compared to EDGs, such that there were no cases in which adversaries disabled TDPs but not EDGs. The probability of CD without a FLEX strategy was calculated by multiplying the sabotage event probability with probability of the design basis system failures obtained from a generic probabilistic risk assessment model. For example, the CD probability for Outcome 5 was obtained from the product of 0.843 and the conditional CD probability of a LOOP event, which was taken as 1E-3 in this case. Meanwhile, the conditional CD probability for Outcome 8 is 1, as shown in Figure 11. Each of the FOF simulation results were imported into EMRALD to evaluate the success likelihood of FLEX strategies. Ten thousand Monte Carlo runs were simulated for each of these FOF results, totaling to three million simulations. The resulting CD probabilities are tabulated in the last column of Table 3. It was found that a FLEX mitigation strategy could significantly reduce the likelihood for a CD and radiological release into the environment due to sabotage attacks by a factor of three. Although the model and data used in this case study are hypothetical, it still serves as a proof of concept for the proposed FOF-FLEX integration and how existing resources in NPPs can be incorporated into the physical security evaluation to improve the plant's safety and security.

Table 3.Results from multiple FOF simulations.

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

4.1.5 FLEX-Thermo-hydraulics Analysis

The core damage timing of one hour described in the previous section is a conservative estimate based on the assumption that all safety systems fail at the same time. In reality, several of the safety systems may operate for a limited time before they fail at different timings. For that reason, this Section provides a more realistic estimate of the time period available before the reactor is damaged by taking into account uncertainties on safety system actuation and operator's performance. These uncertainties are incorporated in the thermal-hydraulic analysis to simulate the plant's response when adversaries are successful in sabotaging all the equipment in the target set. A typical 1000 MW NPP model is simulated in RELAP5 [23]. The reactor is assumed to be running at full power at the time of attack and having a minimum battery backup of 4 hours. Safety systems are in place to bring the reactor to a safe shutdown state when an attack causes an initiating event identified in the PRA model. If automatic signals fails to actuate the safety systems, the reactor operator follows the emergency procedure to recover the mitigation process. The statistical uncertainty of operator action timings is listed in Table 4.

Table 4. Task completion time of operator actions

Task	Average(s)	Standard deviation (s)
Average performance time of standard post-trip actions	196.2	72.8
Event diagnosis time data for SBO	251.7	78.6
Minimizing the leakage from RCS	395.4	61.0
Preventing the over pressurization of main condensers	410.8	76.5
Restoring AC power	515.6	89.7

Aside from uncertainties on human operator actions, there are additional uncertainties on the performance of safety systems and components due to random failures, such as the failure to start and failure to run continuously. These uncertainties are modeled in a static manner in the plant PRA model. However, these uncertainties are incorporated dynamically in the thermohydraulic model in order to estimate the core damage timing. The uncertainty sources and their statistical distributions are listed in Table 5.

Table 5. Uncertainty sources and statistical distributions

Variable	Distribution
Number of Auxiliary Feed Water (AFW) (MDP/TDP) available	Bernoulli (P_f=6.57E-3 / 1.46E-2)
Initiation timings of AFWs	Normal (μ=196.2, σ=72.8)
Offsite power recovery (hr)	Lognormal (μ=0.793, σ=1.982)
Operation of secondary depressurization	Bernoulli (P_f=2.31E-3)
Initiation timings of secondary depressurization	Gamma (α=28.83, β=14.28)
AFW Pump (MDP/TDP) fail to run (hr)	Exponential (λ=3.59E-3/2.21E-3)
Reactor Coolant System (RCS) depressurization operation	Bernoulli (P_f=5.69E-3)
Initiation timing for bleed operation	Gamma (α=4, β=0.03178)
Number of high-pressure safety injection pumps	Bernoulli (P_f=6.66E-4)

RELAP5 input files were populated using the grid-sampling method on the uncertainty sources listed above. The peak cladding temperature (PCT) variable computed by RELAP5 is selected to determine whether the reactor core is damaged or not. Simulation results show that in 993 out of 10800 RELAP5 runs, the reactor core is not damaged. Meanwhile, the timing distribution when the reactor core is damaged is plotted in Figure 24. The figure shows that no core damage occurs in less than one hour, which agrees with the aforementioned explanation that the 1-hour core damage timing is a conservative estimate. Most of the core damage timings are distributed between 1.5 to 2 hours. Core damage that happen beyond 4 hours is caused by the successful recovery of offsite power accompanied by the late running failure of AFW pumps and/or other variables listed in Table 5.

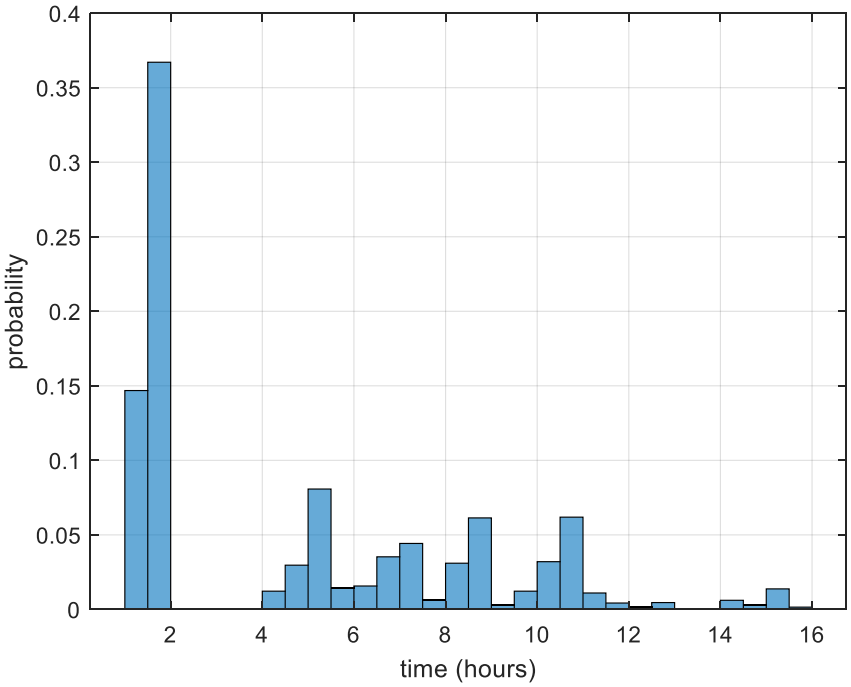
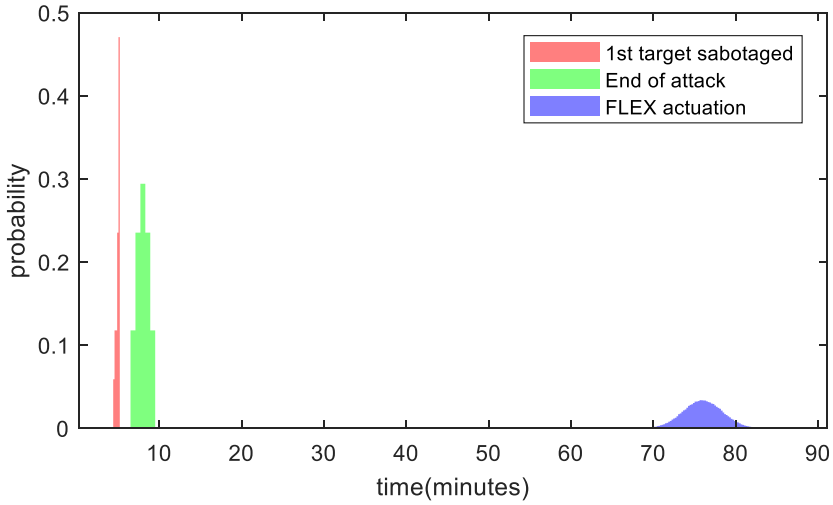
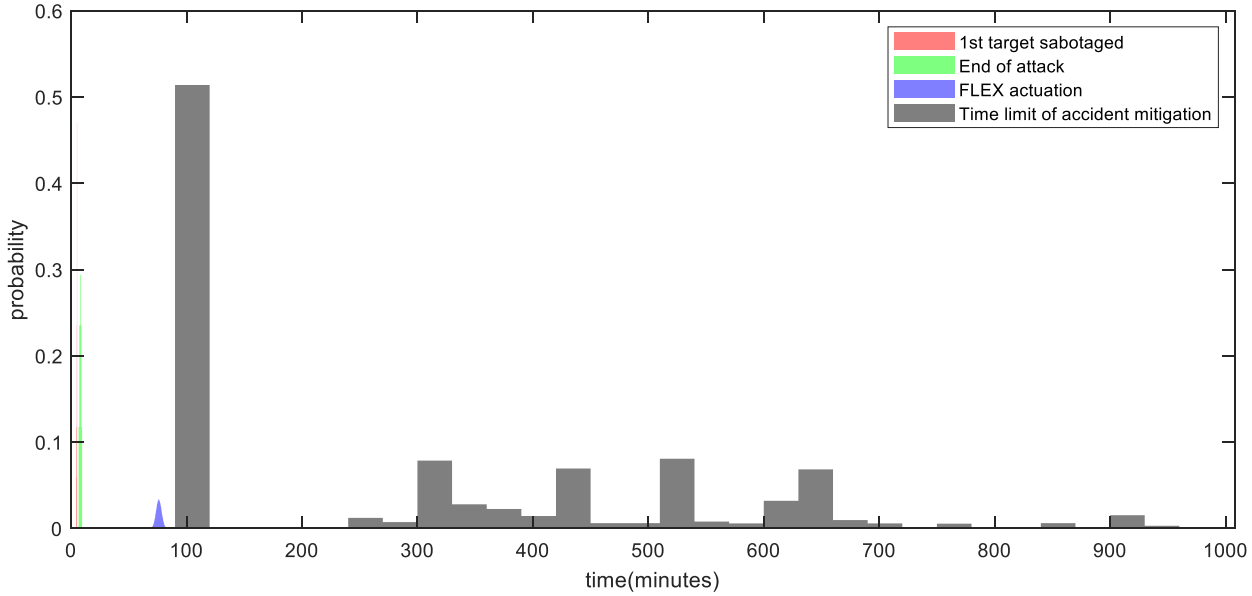


Figure 24. Distribution of core damage times

By using this time distribution, the success probability of the parallel FLEX action model remains the same because the FLEX time distribution does not intersect the 1 hour time limit. A small core damage probability value in the order of 1E-4 exists due to the random failure of components. For the serial FLEX model, all of the FLEX timing distribution estimated by the 300 FLEX-FoF coupled simulations were less than the minimum core damage timing as shown in Figure 25. This result indicates that the sequential FLEX strategy may be sufficient in mitigating the adverse effects of adversary attacks. It is important to note however that the data in this example, i.e., FLEX procedure, facility layout, attack scenario and FLEX timing data are not actual data from a nuclear power plant and therefore the results may not be directly applicable to nuclear power plants. However, this case study illustrates the methodology that nuclear power plants can adopt to evaluate their physical protection system by crediting operator actions in mitigating the adverse effects of a sabotage attack. The operator actions include actions using the design basis safety systems and FLEX mitigation strategies supported by thermal-hydraulic analysis of the plant's response.



(a) FoF-FLEX timeline



(b) FoF-FLEX timeline compared to the core damage timing from thermal-hydraulic simulations

Figure 25. Time distribution of FLEX actuation and core damage

4.2 Location Optimization of Bullet-Resistant Enclosures

This section explains about the use of EMRALD model to optimize the placement of an additional Bullet-Resistant Enclosure (BRE). The facility layout is shown in Figure 26, where six BREs are shown with letters from A to F. In this case study, there exists a need to install an additional BRE aside from the existing six BREs as a redundant measure. The objective of this study is to identify the optimal location for the additional BRE. A total of 7 candidate BRE locations were selected as indicated by the numbers 1 to 7 in the figure. The challenge in this study is that when the initial PPS configuration is already effective in protecting the target sets, adding a redundant PPS element such as BRE may not result in a noticeable increase in P_E. In order to observe the change in PE, the analyst may need to significantly increase the

number of FoF simulation runs. This approach is not efficient since the FoF simulation requires a significant computational power and time.

In order to alleviate such difficulty, EMRALD was utilized to perform a simulation that identifies and disables the most effective BRE, substitutes it with the redundant BRE candidates, and evaluating the new PPS effectiveness. This method creates a deficiency in the PPS posture intentionally such that the change in P_E of the modified PPS can be analyzed without significantly increasing the simulation count.

Figure 26. Facility layout

4.2.1 BRE-Optimization Analysis

The EMRALD model created for this case study is shown in Figure 27. The model starts by initializing the variables, and identifying the most effective BRE. The "Find_Best_Guard_Once" State runs the FoF simulation for 100 times, reads the FoF output file, and identifies the BRE which neutralizes adversaries the most. This State is executed only once. If no such BRE is found, the simulation activates the "No_Best_Guard_Found" State which will terminate the simulation. If the most effective BRE is found, the "If_Best_Guard_Set" Event is triggered and the simulation flow will be transferred to the "Substitute_Best_Guard" State. This State modifies the FoF input files by writing the best BRE in the Ignored list and removing each of the BRE candidates from this Ignored list. This State produces 7 scenarios where each scenario is run 100 times by taking into account FoF uncertainties. The "Run_Loop" State executes these scenarios, extracts the results and tabulates them for comparison. After all scenarios have been simulated, the simulation ends.

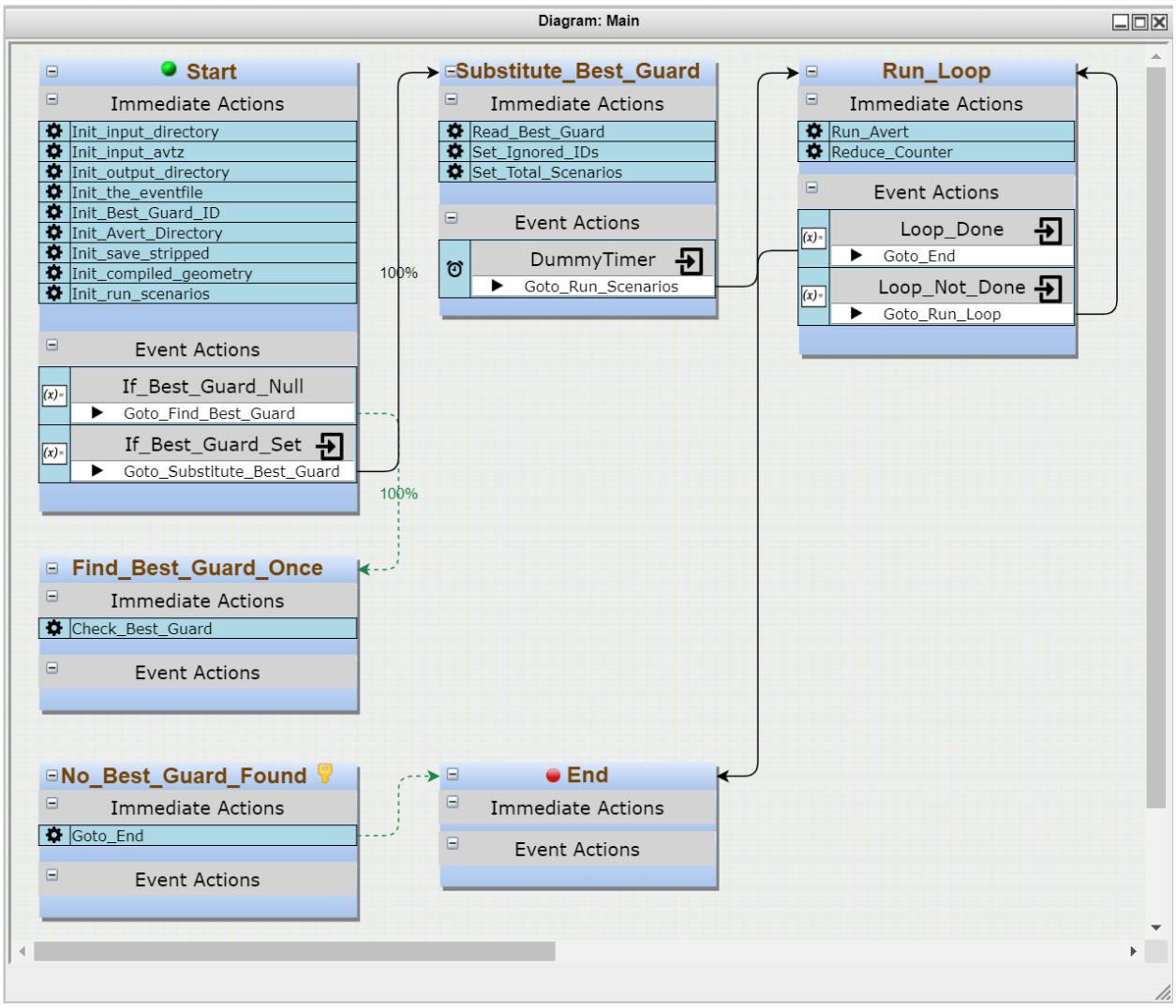


Figure 27. EMRALD Model

The Actions in an EMRALD model may contain C# scripts to execute complex simulation tasks. Figure 28 shows the C# code in the "Check_Best_Guard" Action within the "Find_Best_Guard_Once" State. This code calls an external custom function Extract_Best_Guard_ID.exe by passing the necessary arguments, i.e., the path of input and output directories. It then fetches the output of the code in the postprocessing block. The code waits for Extract_Best_Guard_ID.exe to complete its execution and finds the output file named Readme.txt. If the file is not found, the code informs EMRALD to switch to the "No_Best_Guard_Found" State. Meanwhile if it is found, EMRALD activates the "Substitute_Best_Guard" State. This Action imports global variables from the model as shown in the figure, i.e., input_directory, input_avtz as the input file name, output_directory, and the_eventfile as the output filename.

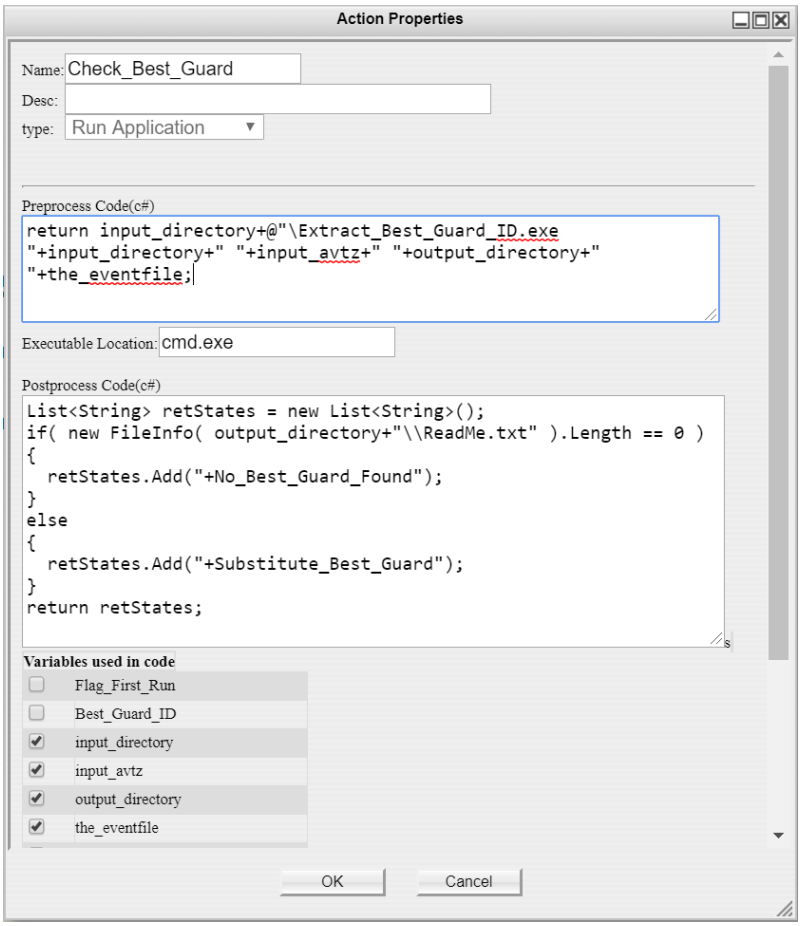


Figure 28. EMRALD code for the "Check_Best_Guard" action

EMRALD code for the “Read_Best_Guard” Action is shown in Figure 29. The first conditional statement evaluates whether the Best_Guard_ID is initialized in the “Start” State, which may be identified from a separate FoF simulation. This initialization is beneficial to reduce EMRALD simulation time. If the variable is not initialized, the code reads the first line of the Readme.txt output file generated from the “Check_Best_Guard” Action and assigns it to the global “Best_Guard_ID” variable. This first line of the file contains the unique ID number of the most effective BRE.

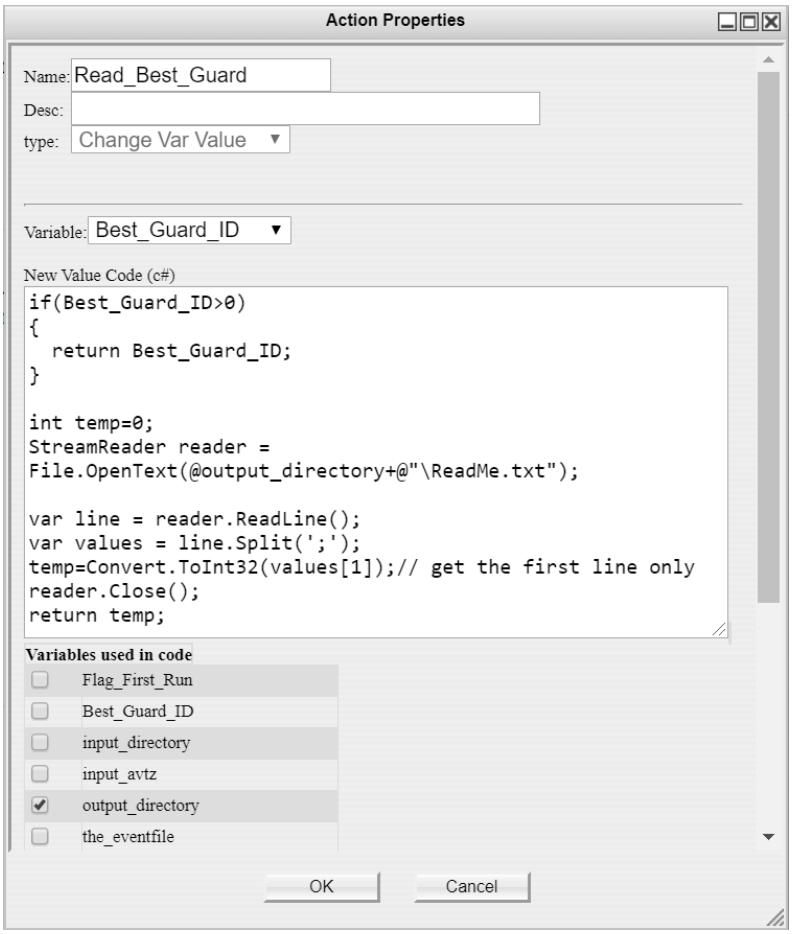


Figure 29. EMRALD code for the “Read_Best_Guard” action

The part of EMRALD code for the “Set_Ignored_IDs” Action is shown in Figure 30. This code reads a list of unique ID numbers stored in the BRE_IDs.txt file. The first iteration in the code extracts the IDs of BRE candidates and stores them in a variable array. The second iteration walks through the array variable and writes multiple text files which list the BRE IDs to be excluded from the FoF simulation. Each list comprises six BRE candidates and the most effective BRE. The code saves the total number of scenarios as Num_Scenarios.

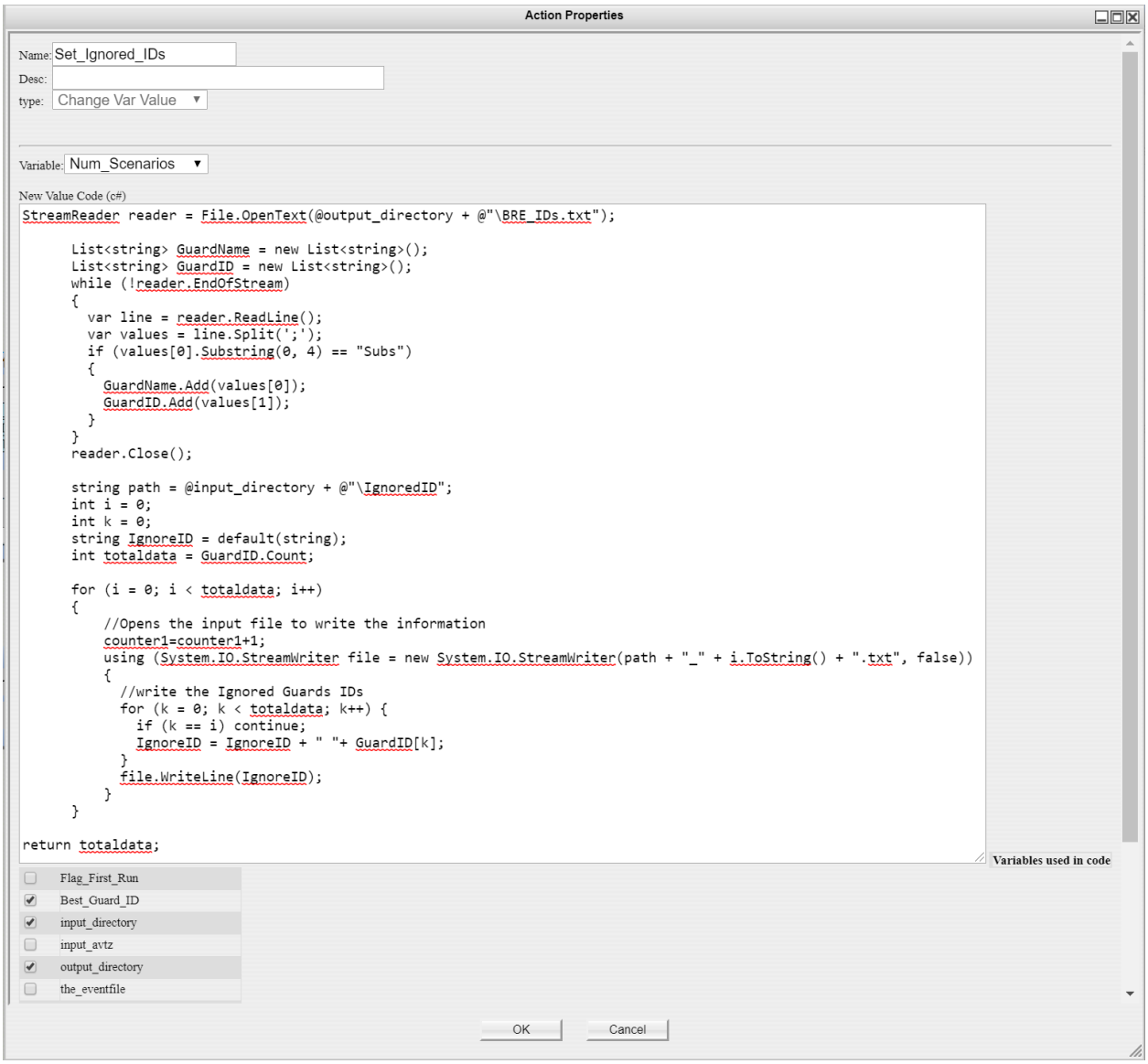


Figure 30. EMRALD code for the "Set_Ignored_IDs" action

The “Run_Avert” Action shown in Figure 31 executes the FoF scenarios generated by “Set_Ignored_IDs” Action sequentially. Its Preprocess code fetches the filenames of FoF scenarios and runs AVERT FoF software for each of the scenario. The Postprocess code waits until AVERT simulation is completed, fetches AVERT output file, renames and moves it from the working directory into a consolidated result directory. EMRALD then reads and extracts the PE value from this output file, and writes it into an output summary text file named “all_results.txt”. The “Run_Loop” State iterates this action iteratively until all scenarios have been simulated. Therefore, the summary text file contains the PE values from all scenarios.

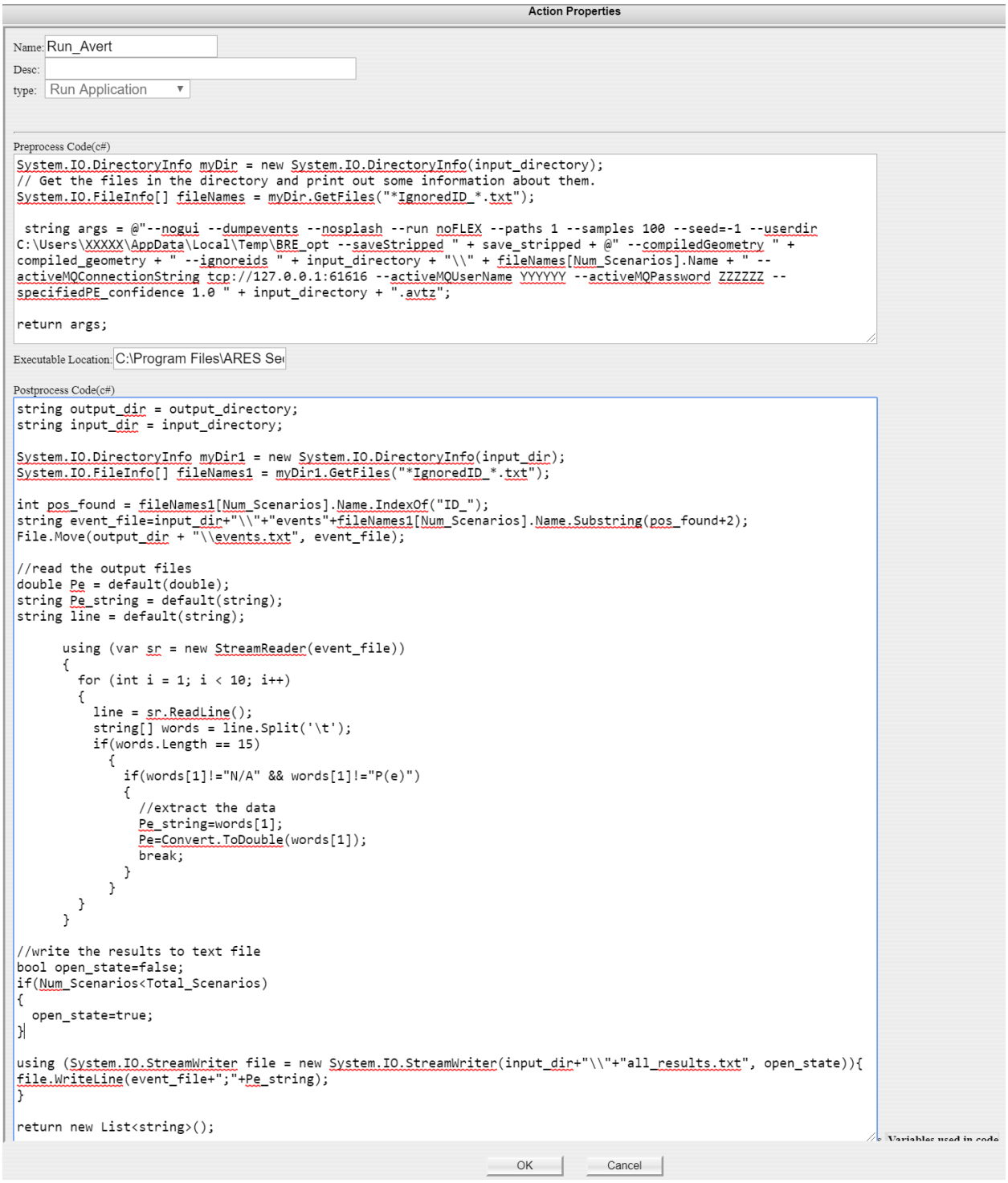


Figure 31. EMRALD code for the "Run_Avert" action

4.2.2 Results and Discussion

Results of the EMRALD simulation are shown in Table 6. The initial PPS configuration having all the guards posted in BRE location A to F has a P_E of 0.99. This result implies that there is only 1 run out of 100 simulation runs in which the adversaries managed to sabotage all of the target sets. In order to

observe any effect from the additional BRE, the simulation runs may need to be increased to 1000 or more for each of the BRE candidates. This approach is computationally demanding and is not time-efficient. By combining the FoF simulation tool with EMRALD, the whole simulation was completed with 700 runs instead of several thousand runs. The EMRALD model identified BRE B as the most effective post and removed it from the simulation. This process allows for a Defense-in-Depth analysis to find the optimal location for the additional BRE. As the Table suggests, the optimal location for the additional BRE is BRE number 3 when BRE B is removed.

Table 6. EMRALD results

BRE	P_E
Initial configuration	0.99
BRE 3	0.98
BRE 1	0.97
BRE 2	0.96
BRE 4	0.84
BRE 6	0.87
BRE 7	0.82
BRE 5	0.82

This process used to evaluate the BRE location helped to develop the process for "Potential Strategy Evaluation" discussed in section 3.2. Although this process was used to evaluate BRE locations, other equipment or personnel optimization could use the same strategy. For example, expert judgement and facility planning could determine location options for a remote weapon and this method could be used to pick the most beneficial location. Then the best option can be used to evaluate a guard reduction as described in section 3.3.

5. CONCLUSION AND FUTURE WORK

This report describes the research and development being performed at INL towards a dynamic modeling and simulation framework to enable physical security optimization at commercial nuclear power plants. The framework is based on the dynamic modeling tool EMRALD and is demonstrated for applications that can result in physical security optimization. Two main applications are presented: 1. Integrating FLEX portable equipment performance with FOF models of a plant's physical security posture, and 2. Location optimization of bullet resistant enclosure.

The generic framework for modeling FLEX portable equipment is described in detail, followed by a case study modeling an adversarial attack aimed at causing a radiological release by sabotaging the plant's power supply and its ultimate heat sink capabilities at a hypothetical PWR. Two distinct FLEX deployment strategies, series and parallel, are modeled with distinct timelines. The results of the adversarial attack modeled in a commercial FOF tool, AVERT, are integrated with the FLEX deployment model in EMRALD. Monte Carlo simulation is used to model the distribution of the timeline in FLEX deployment strategies. Thermal-hydraulic analysis of FLEX performance is performed in RELAP5 and integrated with the EMRALD simulations to provide more realistic timelines in the models.

The results demonstrate that, even in the extreme case of a successful adversarial attack, deployment of FLEX equipment can result in a significantly high likelihood of preventing radiological release. The modeling and simulation framework of integrating FLEX equipment with FOF models enables the NPPs to credit FLEX portable equipment in the plant security posture, resulting in an efficient and optimized physical security.

The objective of location optimization of BRE is to determine the best location in the plant for a new BRE being planned by the plant to enhance their physical security effectiveness. The plant physical security FOF model is integrated with EMRALD that performs Monte Carlo simulation to run different attack scenarios and a discrete set of potential BRE locations. Sensitivity analysis is used to determine the most effective location for the BRE. The optimization approach can be extended to wide applications such as location optimization of remotely operated weapons and other strategic fixed assets.

Ongoing and future efforts in this area include: 1) Implement the framework on a plant's specific physical security posture and FLEX equipment; 2) Integrate with other commercial FOF tools, such as Simajin. The INL team has engaged with the vendor of Simajin, RhinoCorps, for this integration; 3) Model the FLEX equipment and enclosure as a target set in the physical security posture, and 4) Integrate human reliability analysis in the dynamic model.

6. REFERENCES

1. Pacific Gas & Electric Company, "PG&E Company 2018 Nuclear Decommissioning Costs Triennial Proceeding Prepared Testimony – Volume 1," December 13, 2018. https://analysis.nuclearenergyinsider.com/pge-seeks-decommissioning-head-start-cost-estimates-rise.
2. NRC. 2012. *Issuance of Order to Modify Licenses with Regard to Requirements for Mitigation Strategies for Beyond-Design-Basis External Events*, EA-12-049, Washington, D.C: U.S. NRC.
3. United States Nuclear Regulatory Commission. "Emergency Preparedness in Response to Terrorism." https://www.nrc.gov/about-nrc/emerg-preparedness/about-emerg-preparedness/response-terrorism.html#one.
4. United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73. "Physical Protection of Plants and Materials." https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/.
5. United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73, Section 55. "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage." https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0055.html.
6. Garcia, Mary Lynn. 2005. *Vulnerability Assessment of Physical Protection Systems*. Elsevier.
7. Nuclear Energy Institute. 2017. "Guidance for Optimizing the Use of Portable Equipment," NEI 16-08, Washington D.C.
8. Idaho National Laboratory. "Event Modeling Risk Assessment using Linked Diagrams (EMRALD)." https://emrald.inl.gov/SitePages/Overview.aspx.
9. 2020. "AVERT Physical Security." Ares Security Corp. https://aressecuritycorp.com/avert.
10. RhinoCorps Ltd. Co, "Simajin: Simulation Application Suite", https://www.rhinocorps.com/products/simulation-application-suite/, retrieved September 14, 2020.
11. Kang, D., & Chang, S. 2014. "The safety assessment of OPR-1000 nuclear power plant for station blackout accident applying the combined deterministic and probabilistic procedure." *Nuclear Engineering and Design vol. 275*, 142–153.
12. Nuclear Energy Institute. 2016. "NEI 12-06 Rev. 4: Diverse and Flexible Coping Strategies (FLEX) Implementation Guide." Washington, D.C.: NEI.
13. U.S. Nuclear Regulatory Commission (NRC). "Nuclear Power Plants Security Assessment Standard Set of Scenarios," December 20, 2007.
14. Whitehead, D. W., C. S. Potter, and S. L. O'Connor. "Nuclear power plant security assessment technical manual." Sandia report SAND2007-5591 (2007)
15. Electric Utility Cost Group, https://www.eucg.org/.
16. Osborn D., et. al. "Joint INL/SNL Physical Security Evaluation", INL/LTD-19-55901, September 2019.
17. L. Kull, L. Harris, Jr., and J. Glancy, VISA—A Method for Evaluating the Performance of a Facility Safeguards System, in Proceedings of the Eighteenth Annual Institute of Nuclear Materials Management, Inc. Meeting, held in Washington, D.C., June 29 – July 1, 1977, in Institute of Nuclear Materials Management, vol. 6, no.3, pp.292-301, Fall 1977.

18. United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73, Section 1. “Purpose and Scope.” https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0001.html.
19. United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 50, Section 54. “Conditions of Licenses.” https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0054.html.
20. Nuclear Energy Institute. 2017. “Guidance for Optimizing the Use of Portable Equipment,” NEI 16-08, Washington D.C.
21. NEI, NEI 12-06 Rev.4: “Diverse and Flexible Coping Strategies (FLEX) Implementation Guide”, Nuclear Energy Institute, Washington DC, 2016.
22. Kang, D., & Chang, S. 2014. “The safety assessment of OPR-1000 nuclear power plant for station blackout accident applying the combined deterministic and probabilistic procedure.” *Nuclear Engineering and Design vol. 275*, 142–153.
23. Shah, A.U.A.; Christian, R.; Kim, J.; Kang, H.G., “Coping Time Analysis for Chromium coated Zircaloy for Station Blackout Scenario based on Dynamic Risk Assessment”, Proceedings of The 15th Probabilistic Safety Assessment and Management Conference (PSAM 15), Venice, Italy, November 2020.

Appendix A
Physical Security Working Group Meetings

September 2019 Meeting

The LWRS Program Physical Security Pathway held the first meeting of the Physical Security Stakeholder working group on September 10-12, 2019 at Sandia National Laboratories. This working group is comprised of nuclear enterprise physical security stakeholders and the meeting included over 10 Utilities representing roughly 60 nuclear power plants, two staff from the Nuclear Regulatory Commission, physical security vendors, the Nuclear Energy Institute, the Electric Power Research Institute, and staff from Sandia National Laboratories and Idaho National Laboratory. Following is the overview and the findings and priorities identified from the meeting with any sensitive items removed.

Overview

A high-level summary of each briefing and the main presenter(s) is provided.

LWRS Overview – Bruce Hallbert, LWRS National Technical Director, INL

- Discussion on the history and current mission of the DOE-NE Light Water Reactor Sustainability (LWRS) Program. A presentation of the each of the LWRS pathways was given as well as the new initiatives such a physical security.

Overview of Physical Security Pathway Program Plan – Mitch McCrory, LWRS Physical Security Initiative, SNL

- Discussion on the motivation and current efforts of the LWRS PSI. The motivation for the LWRS physical security working group and the makeup of the stakeholders was also presented.

LWRS PSI Working Group Charter Review – Mitch McCrory, LWRS Physical Security Initiative, SNL

- A review of the working group charter was conducted. Edits, changes, and questions were to be given to Jodie Lord (SNL).

NEI Security Working Group Update – David Young, Nuclear Security and Incident Preparedness Technical Advisor, NEI

- An overview of the current NEI efforts on physical security was given. A discussion on NEI's priorities and where DOE could provide assistance (e.g., unattended openings) was conducted.

NRC Discussion on Physical Security Regulatory Status and Needs – Michele Sampson, Reactor Security Branch Chief, NRC

- An overview of current NRC efforts and guidance for physical security was given. A discussion on recent regulatory guidance (e.g., security bounding time) was conducted.

Sandia National Laboratories Overview – Sylvia Saltzstein, Nuclear Energy Safety and Security, SNL

- A corporate overview and general discussion of Sandia's capabilities was given. This discussion also included a review of the Sandia mission areas which were assisting with the LWRS PSP.

Overview of INL Physical Security Research – Vaibhav Yadav, LWRS Principal Investigator, INL

- A presentation of the current INL efforts for the LWRS PSI was given. Stakeholder feedback was provided.

HAZCADS – Doug Osborn, Int'l Nuclear Security Engineering R&D S&E, SNL

- A discussion was held on the need for a novel solution to nuclear security risk assessment through the integration of various risk methods. HAZCADS is an example of this by leveraging advantages of PRA and System Theoretic Process Analysis.

EMRALD – Steve Prescott, Software Analysis/Integration Engineer, INL
- A presentation of the dynamic PRA software was held. An example of using EMRALD's capabilities was discussed; the risk associated with response force using the restroom.

International Nuclear Security – Jordan Parks, Int'l Nuclear Security Engineering R&D S&E, SNL
- An overview of the new NNSA initiative to collaborate with international nuclear power plants on security (cyber and physical) was given.

ROWS Presentation – Kristopher Klingler, High Consequence Robotic Systems Manager, SNL
- An overview presentation and discussion regarding ROWS technology was given. Discussions of how the domestic nuclear power fleet could leverage this body of work was held. A facility tour was conducted.

INL Nuclear Cyber Research – Shannon Eggers, Cybercore, INL
- An overview of INL's nuclear energy cyber research was held. A discussion on the possibility of a combined DOE cyber-physical security work group was held; such a meeting from time to time would be appropriate.

Sandia Cyber – Lon Dawson, Energy Security R&D S&E, SNL
- An overview of SNL's nuclear energy cyber research was held.

Deliberate Motion Algorithms and Water Intakes – J.R. Russell, Technology Development R&D S&E, SNL
- A discussion was held on recent SNL efforts on sensor data fusion to develop deliberate motion algorithms and how this technology could be applied at domestic NPPs. A discussion on SME operational experience and technical solutions was conducted on water intakes.

Access Delay Tech Transfer Volume II – Chad Monthan, Access Delay and Structural Assessment Manager, SNL
- Discussions and a demonstration were held on the use of the Access Delay Tech Transfer Manual Volume II and how to create detailed timelines (e.g., complexity factors). A discussion on application of uncertainty to barriers was also held.

Cyber Security Threat Brief – John Mulder, Critical Infrastructure Systems, SNL
- Discussions on recent cyber events was held

UAS VA Brief – Chris Faucett, Severe Accident Modeling and Analysis, SNL
- A presentation of the SNL work supporting NRC's vulnerability analysis from UAS was given.

Human Factors/Reliability Threat Modeling – Jason Morris, Human Factors R&D S&E, SNL
- A presentation of efforts on cognitive modeling for threat was given.

Threat Modeling – Ray Trechter, Interactive System Simulation and Analysis Manager, SNL
- A discussion on SNL's capabilities in adversary and ROWS modeling was given.

General Notes

The following list of general notes which were taken;

- Unattended opening is a priority
  - 2D vs 3D requirements
- Taking credit for ROWS
- Definition, verification, validation, and NRC approval of performance measure
- Potential pilot for demonstrations
  - ROWS, data fusion, water intakes
- Identifying pilot for going below regulatory requirements using 10CFR 50.90
- 1-year and 2-year milestones to successfully achieve 3+ year mid-term priorities
  - Stakeholder inputs from LWRS working group
- Review of NRC SECY-19-0055
  - Crediting operator actions and law enforcement response
  - Why not credit off-shift response force?
    - Akin to other off-shift personnel manning the TSC
    - MOU with local law enforcement to 'borrow' a bearcat to return
- Review of NEI Security Bounding Time
- Adversary travel speeds
  - Review of DOE data, and methods for achieving site-specific data
- Identify synergy between Physical Security and other LWRS pathways
  - RISA, and Plant Modernization
- Drones for patrolling
  - Limitations are with FAA
- Deliberate motion algorithm, data fusion
- Developing knowledge repository at utilities for FoF models, etc.
  - Leverage DOE deep-dive training and workshops on physical security
- Paradigm breaking solutions for relief in everyday task
  - Access control, vehicle inspection
- Sabotage requirement to consider time to irreversible core damage
  - Could better define this out to in-vessel retention or beyond Zirconium metal oxidation
- Consider diminishing adversary capabilities over time
- Review NRC Reg. Guide 5.81
  - Consider including operator actions outside of the control room, FLEX, etc.
- Dynamic analysis will need to be piloted with a known problem
  - A practical bench test

Detailed Notes

The following are the detailed notes which were taken.

Credit for Active Protection Measures

Develop methodology to determine adversary timelines;

- Adapt and enhance material in NUREG/CR-7145
- Include criteria for adversary travel speeds
- A manual for method and standards using computer modeling
- Methodology should recognize that an adversary timeline may end in neutralization of the adversary
- Establish standards for probabilities of interruption & neutralization (P_I & P_N in NUREG/CR-7145)

Final product should have both a technical basis section and an implementation section with instructions and worksheets appropriate for use by a site target set analyst in the application of Security Bounding Time (SBT)

Credit for law enforcement tactical support to enable operator actions/SBT

Methods to identify target sets where credit for an SBT may be practical

- Times to fuel damage will permit performance of a post-SBT operator action to prevent damage
- Assumptions, case boundaries and simplified approaches for use by site target set analysts
- Identify post-SBT operator actions to include within target sets
- Actions to prevent or mitigate the loss of a target element

Unattended Openings and Protected Areas

Make existing research and testing documentation available to licensee personnel

- Document review may provide a technical basis for a limiting 3-dimensional pathway size
- If needed, conduct additional testing on various pathway sizes and configurations
- Coordinate tests with NRC and licensees to ensure development of useful data

Performance-Base Testing Requirements

Develop a technical basis for using performance/reliability data to inform security equipment testing requirements (e.g., IDS, contraband detection, etc.).

- Include a template/procedure that a licensee could follow for how to use their data to generate new performance-based testing requirements

AI-Driven ROWS

Longer-term action – something like the Samsung SGR-A1.

This first-time meeting between utilities, vendors, NRC, and DOE physical security experts generated a lot of excitement around near-term potential that the LWRS Program can have on physical security for the nuclear industry stakeholders. The working group agreed that they would like to have two stakeholder meetings a year initially and a follow up meeting in November 2019 to further explore ideas generated. The November meeting will provide input to the PSP as we head in to FY20 and prioritize tasks. The working group also provided a venue for connections to be made on LWRS pilot programs and collaborations.

November 2019 Meeting

During the November 2019 meeting, a series of presentations and discussions were held over the course of two days. This section provides a high-level overview of the discussions and a list of the presentations which can be provided to the meeting attendees.

Overview

Welcome to ORNL –

Mehdi Asgari, LWRS Deputy Director, ORNL and Cary Crawford, Group Leader, Safeguards & Security Tech

LWRS Physical Security Pathway Update

Stakeholder Inputs on Priorities FY20 current work package overview

- Project Management/Working Group – Mitch McCrory
- Advanced Security Technologies – Kris Klingler
- Dynamic Risk Framework – Shawn St. Germain
- Risk Informed Technologies – Doug Osborn
- Plant Physical Security Cost Drivers – Shawn St. Germain

Working Lunch Stakeholder Inputs on Priorities

Timelines and Feedback

Other DOE-NE Funding Opportunities
FOA, SBIR, GAIN, NSUF, etc.- Shawn St. Germain

NEI Working group update
Bill Gross, Director Incident Preparedness, NEI

Wrap up
Alignment with LWRS Physical Security Pathway R&D Goals – Mitch McCrory
Suggestions for next LWRS Working Group meeting

ORNL Presentations of Physical Security Capabilities
Y-12 VA & Security Modeling Efforts – Eric Bishop, VA and modeler, Y-12, (UCNI)
VISAC Software – Dave Sulfredge, Technical Staff, ORNL, (UCNI)
Current DOE Thoughts on Designing a Protection Strategy – Commie Byrum, ORNL, (UCNI)

Scribe 3D-EMRALD Dynamic Modeling
Steve Prescott, INL

Closing Remarks
Jeffrey Johnson, Nonproliferation R&D Integration Manager
Coordinated R&D to counter nuclear terrorism. Looking for demonstrations for ICONS at the government booth in Feb. – Scribe 3D

Notes and Feedback

- Have we already looked at what is used in DOE complex for standards and metrics?
- Water intake pilot with TVA and Dominion.
- Not a ton of interest on recall for takebacks.
- How do we leverage counter UAS R&D from Department of Defense and DHS to be prepared when threat and legislation catches up domestically?
- Does measure of effectiveness research include future design? Yes, already does.
- Does the charter include addressing rule changes? Doesn't exclude it. Why bother when there are other ways around it with a technical basis.
- What are the security working groups priorities going forward? UAO's, adversary timelines, DMA, came up as worth focusing on. NEI will help identify which solutions will need their advocacy go forward and interface on policy and the broader working group.
- Would like to identify a clear problem statement and milestones and help set LWRS up for success as an advocate.
- Two problems when looking at adversary timelines. The paper version is different than FoF -need to have common methodology or distribution, maybe we should move to models.
- Are we missing anything here? Things that don't cost capital on the behalf of utility are best to focus on like operator timelines, responder timelines, flex equipment etc. – can be done in short term at no cost. How to program risk tool pilots to make sure the use case is a cost effective one and tangible benefit.
- Currently have models but need guidance on which data and how to use it.
- How are you going to get the new tools accepted? Some already are, others will need to bring NRC along, some will require an independent evaluation by the NRC.
- Clarify "at all times" language in 10CFR-73.55 – Can it allow for avoiding an X+1 on rotations coverage etc? Can we show what the effects are through modeling to provide the answer.
- NRC says that modeling has to be valid to be accepted.

June 2020 Virtual Meeting

The working group meeting for spring 2020 was originally planned to be held in March 2020. Due to the travel restrictions imposed due to COVID-19, the meeting was delayed. On realization that normal travel would not be resuming soon in summer 2020, the working group meeting was organized over audio-video conferencing in the month of June. Three web sessions of 2.5 hours each were organized at SNL over three days, June 23rd, 25th, and 30th. The web sessions had a strongly encouraging attendance of over 80 individual attendees spanning stakeholders from the industry, EPRI, NEI, NRC, vendors and national laboratories. While the high attendance was encouraging, the feedback session in the web-based meeting had much fewer inputs and feedback from the stakeholders, compared to a physical meeting. The LWRS PSP team feels that in future, physical meetings would be ideal in order to receive best inputs and feedback. Following is the overview of the webinar:

Tuesday, June 23, 2020

Light Water Reactor Sustainability Welcome

Alison Hahn, LWRS Federal Program Manager, DOE NE

Bruce Hallbert, LWRS National technical Director

LWRS Physical Security Pathway Overview

Mitch McCrory, LWRS Physical Security Program Pathway Lead

- Pathway high-level overview
- Upcoming dates
- Collaboration Projects
- Other security related topics (advanced reactor security, etc.)

Physical Security Pathway 2020 Project Review

Dynamic Risk-Informed Progress

Shawn St Germain, INL PSP Technical Lead

Risk-Informed Adversary Timelines

Dusty Brooks and Andrew Thomas, SNL PSP

Thursday, June 25, 2020

Overview of Day 1 Discussions

Mitch McCrory, LWRS Physical Security Program Pathway Lead

Physical Security Pathway 2020 Project Review (Continued)

Advanced Security Technologies (ROWS) Progress

Kristopher Klingler and Ron Simon, SNL

Adversary Timeline and Access Delay Manual Discussion

Chad Monthan, SNL

Security Cost Modeling

Pralhad Burli, INL PSP

International Nuclear Security (NNSA) Program Overview

Doug Osborn, SNL

Concluding Discussion

Tuesday, June 30, 2020

Overview of Day 2 Discussions

Doug Osborne, SNL PSP Technical Lead

Stakeholder Input: Roundtable Discussions

EPRI, NEI, NRC

DOE-NE Advanced Reactor Safeguards Program Overview

Ben Cipiti, National Technical Director, Advanced Reactor Safeguards

Utility Discussion: Security Challenges and Needs

Future PSP Projects: Discussion on Needs and Impacts

Concluding Discussion

Next meeting; other items.