Methods for Including Mitigation Actions and Plant Behavior into Physical Security for Optimization - Initial Outcomes

Steven R. Prescott[1], Robby Christian[1], S Dan McCorquodale[2], Vaibhav Yadav[1], Shawn W. St Germain[1]

[1]Idaho National Laboratory, Idaho Falls, ID
RhinoCorps, Albuquerque, NM

ABSTRACT

Existing physical security evaluations often define the win criteria associated with adversaries achieving their objective(s). There is a desire to add additional features, such as operator procedures, or after-attack mitigation options, such as FLEX equipment, but these are currently limited because methods to easily evaluate these factors have not been not available or are difficult to validate and credit. Additionally, fixed data for the thermal hydraulics is typically used in determining core damage, where it would be optimal to account for when pieces of equipment are hit versus attack detection time. A less conservative approach accounting for these factors can make a significant difference in whether attack scenarios cause core damage to a plant and could allow for a reduction in security force.

Recent work in the Light Water Reactor Sustainability program has proposed and developed a more inclusive method to model, simulate, and verify the use of operator procedures, force-on-force simulation, and thermal hydraulics, using a dynamic framework. This method is called MASS-DEF (modeling and analysis for safety and security using dynamic EMRALD framework). This paper discusses developing a generic model and the general insights obtained by applying the model and MASS-DEF method to a U.S. nuclear power facility's physical security plan.

Keywords: EMRALD, physical security, modeling

1. INTRODUCTION

The Department of Energy has established the Light Water Reactor Sustainability program to support the continued operation of nuclear power plants (NPPs) in the United States amid the competitive energy market. One of the efforts in the Light Water Reactor Sustainability program is the physical security pathway, which aims to optimize physical security posture in terms of effectiveness and costs through modeling and simulation, applying advanced sensors, and deploying advanced weapons. This work has focused on methods to simulate new defense strategies including operator actions during or after an attack along with a methodology to use the modification to reduce the protection force while showing the new strategy is as good as or better than the current strategy. The work for this paper focuses on an industry pilot to use a dynamic risk model to capture operator procedures and the use of diverse and flexible coping strategies (i.e., FLEX) equipment as an option to mitigate successful attack scenarios. The results of this pilot determined the likely number of guards that could be reduced using a process called MASS-DEF (modeling and analysis for safety and security using dynamic EMRALD framework) [1].

In order for U.S. NPPs to make a security modification under 10 CFR part 50, section 54 [2], they must show the Nuclear Regulatory Commission (NRC) that the changes are equivalent to the existing defense strategy. Additionally, the plant's response force includes the minimum number of armed responders, as required in

10 CFR part 73, and security officers tasked with assigned duties, such as stationary observation, surveillance posts, foot-patrol, roving vehicle patrols, compensatory posts, and other duties, as required [3].

Recently, the NRC outlined the “Reasonable Assurance of Protection Time” concept [4], where if a facility can independently protect against the design basis threat for a minimum of 8 hours, offsite help can mitigate negative outcomes. This emphasizes the value for facilities to accurately evaluate time and mitigation options and is used as a cutoff time for evaluation in this work.

2. METHODOLOGY

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

Facilities have options to include operator actions during an attack and on-site equipment after an attack to help mitigate attack scenarios. This section outlines the development of a dynamic model coupled with the force-on-force (FOF) simulation along with thermal hydraulics tools to allow for more complete modeling capabilities and accurate scenario outcomes.

2.1. Modeling Operator Actions and Use of On-site Equipment

Idaho National Laboratory (INL) has developed the Event Modeling Risk Assessment using Linked Diagrams (EMRALD) [5], a dynamic probabilistic risk assessment (PRA) tool, for other external hazard evaluations. This tool is ideal for modeling and coupling in dynamic safety and physical security evaluations. The INL team developed a generic EMRALD model that imports FOF data, captures general behavior for FLEX use, and functions as a template for specific plant procedures or attack scenarios.

The generic model was designed to use FOF data from an FOF simulation tool, such as Simajin/Vanguard [66] or AVERT [7]. This generic model captures the well-known behavior of a pressurized-water reactor (PWR) to determine whether FLEX equipment could prevent core damage. With the generic nature of the model, the results would not reveal security vulnerabilities, and would not be considered non-public information. The generic model incorporates basic PWR safety elements, such as the control room, diesel generators (DGs), motor-driven pumps, turbine-driven pumps (TDPs), condensate storage tanks, water tanks, etc. Each component is modeled separately with probabilistic transitions between startup, operational, and failed states, along with failure links that come from the FOF simulation data and as informed by the PRA model. All of these components can be set to fail according to the time specified by the FOF results, or if a specific plant does not have the component, such as a second motor-driven pump, it can easily be removed.

Figure 1 shows an example component model for the DG. The StartingDG1 event is a distribution on the time it takes to start up the generator. When the startup demand comes, the generator may start successfully or fail to start. If it starts, the simulation goes to the DG1Running state and transitions to the DG1Failed state if it has random failure or if there is a time set that it is hit by an adversary based upon output from the FOF simulations.

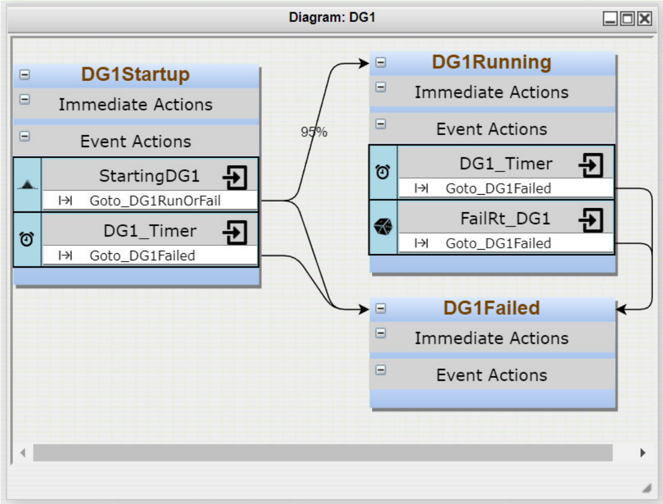
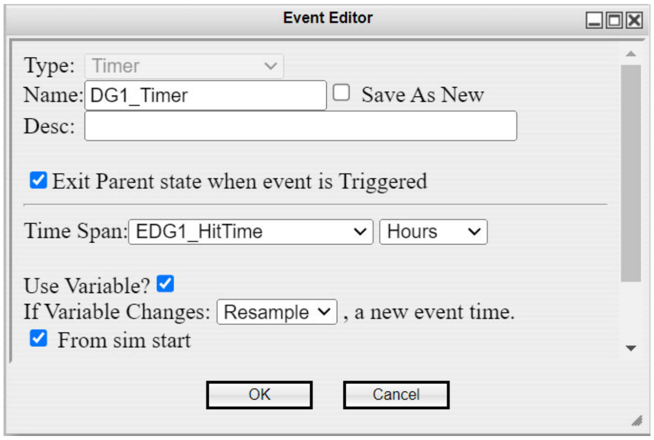


Figure 1. DG operational diagram.

DGs start when offsite power is lost. However, there is a possibility that the adversaries target the generators after they start to operate. The operational status of the generators needs to be monitored. The FOF simulation (Simajin/Vanguard) provides the time data for when the generators are sabotaged. These data are recorded in EMRALD variables EDG1_HitTime and EDG2_HitTime for the first and second generator, respectively. The DG1_Timer event shown in Figure 2 uses this timing variable to switch the generator state from DG1Running to DG1Failed. With this modeling approach, the generators may run for some time before they are sabotaged. This dynamic equipment availability information can be fed into a reactor safety analysis code to evaluate the resulting reactor state.



Type: Timer
Name: DG1_Timer ☐ Save As New
Desc:

☑ Exit Parent state when event is Triggered

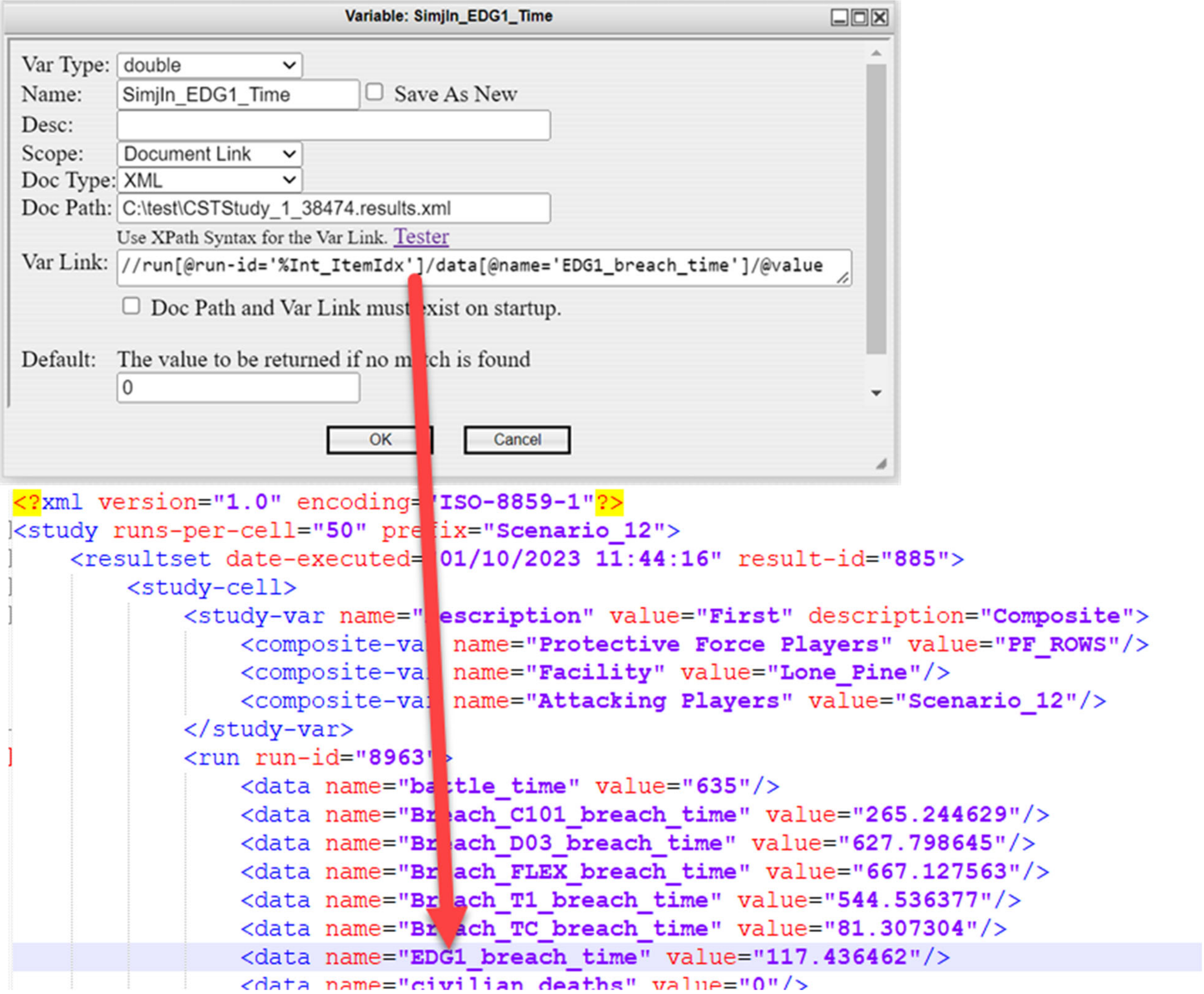
Time Span: EDG1_HitTime Hours

Use Variable? ☑
If Variable Changes: Resample , a new event time.
☑ From sim start

Figure 2. DG1_Timer event in the DG1Running state.

The generic model starts by importing results from an external FOF simulation and extracting the output data. All the critical times, such as when the attack was detected, and target hit times, are read in and set as timers in the EMRALD model. In this pilot, we used RhinoCorps Simajin/Vanguard [66] which outputs results in an extensible markup language (XML) output file. EMRALD provides a method to link variables to data directly in files, Figure 3 shows a sample of this variable linking to an emergency DG's (EDG's) sabotage time. The "Doc Path" field specifies the path to the XML output file, while the "Var Link" field describes the XPath expression needed to extract particular data from the XML file, which, in the case of Figure 3, is the value of EDG1_breach_time data. If EDG1_breach_time data are not found in the XML file, EMRALD returns a default value of 0, which implies that EDG1 is never sabotaged in the attack scenario. To use data from another

FOF simulation tool, similar variables can be linked to result data from that tool for each item that belongs to a scenario target set.



Var Type: double

Name: SimjIn_EDG1_Time □ Save As New

Desc:

Scope: Document Link

Doc Type: XML

Doc Path: C:\test\CSTStudy_1_38474.results.xml

Use XPath Syntax for the Var Link. Tester

Var Link: //run[@run-id='%Int_ItemIdx']/data[@name='EDG1_breach_time']/@value

□ Doc Path and Var Link must exist on startup.

Default: The value to be returned if no match is found

0

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<study runs-per-cell="50" prefix="Scenario_12">
    <resultset date-executed="01/10/2023 11:44:16" result-id="885">
        <study-cell>
            <study-var name="Description" value="First" description="Composite">
                <composite-var name="Protective Force Players" value="PF_ROWS"/>
                <composite-var name="Facility" value="Lone_Pine"/>
                <composite-var name="Attacking Players" value="Scenario_12"/>
            </study-var>
            <run run-id="8963">
                <data name="battle_time" value="635"/>
                <data name="Breach_C101_breach_time" value="265.244629"/>
                <data name="Breach_D03_breach_time" value="627.798645"/>
                <data name="Breach_FLEX_breach_time" value="667.127563"/>
                <data name="Breach_T1_breach_time" value="544.536377"/>
                <data name="Breach_TC_breach_time" value="81.307304"/>
                <data name="EDG1_breach_time" value="117.436462"/>
                <data name="civilian_deaths" value="0"/>
```

Figure 3. XML-linked variable of the EDG sabotage time from Simajin results.

2.2. Operator Procedures

There are two types of operator procedures that can be part of the model. The first set includes actions that could be taken upon detecting an attack. The second set includes actions that could be taken after the attack, and physical security has cleared the site and can support operator movements. In this case study, the facility wanted to evaluate if there was a benefit to filling the steam generator (SG) when an attack was detected as shown in Figure 4. Typically, they run at near 20% capacity and would fill up to 80% after tripping the reactor which would allow for significantly more time to cool the reactor if needed given a successful attack on applicable target components.

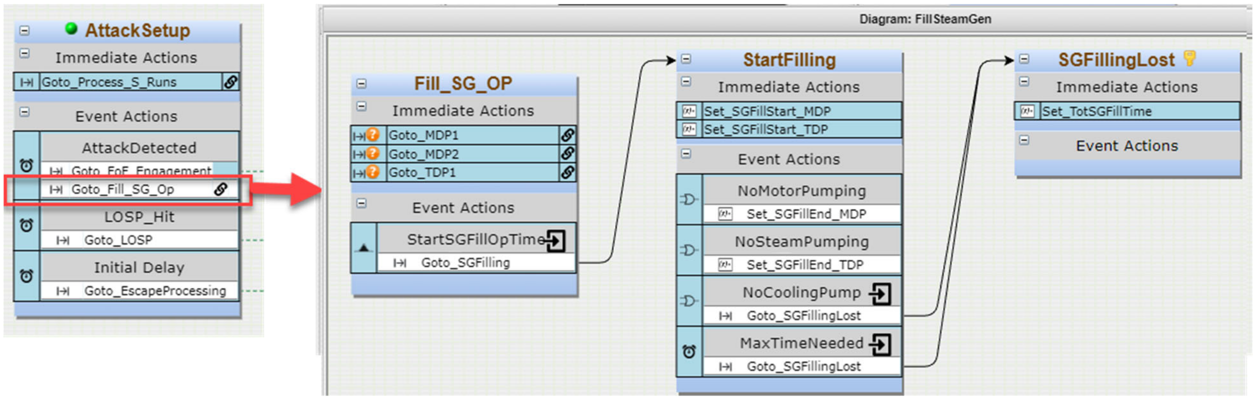


Figure 4. (Left) attack detection triggering evaluation of the EMRALD diagram (right) of the procedure to fill the steam generator after detecting an attack.

The post-attack mitigation actions are modeled as shown in Figure 5. The generic model allows for multiple options on how to cool the plant if cooling is needed. First, the model evaluates if cooling is needed; then, it tries the following options in this order: manually operating the TDP, injecting fire water, using the fire protection pump inside the protected area (PA), dispatching a fire truck, and finally using a FLEX pump. The first option that has the available equipment is used. If required equipment or connections are sabotaged or set as not available by the modeler for the specific facility, then it moves to the next option. For the pilot, both manual operation of TDP and a protection pump, highlighted in red, were enabled as mitigation cooling options.

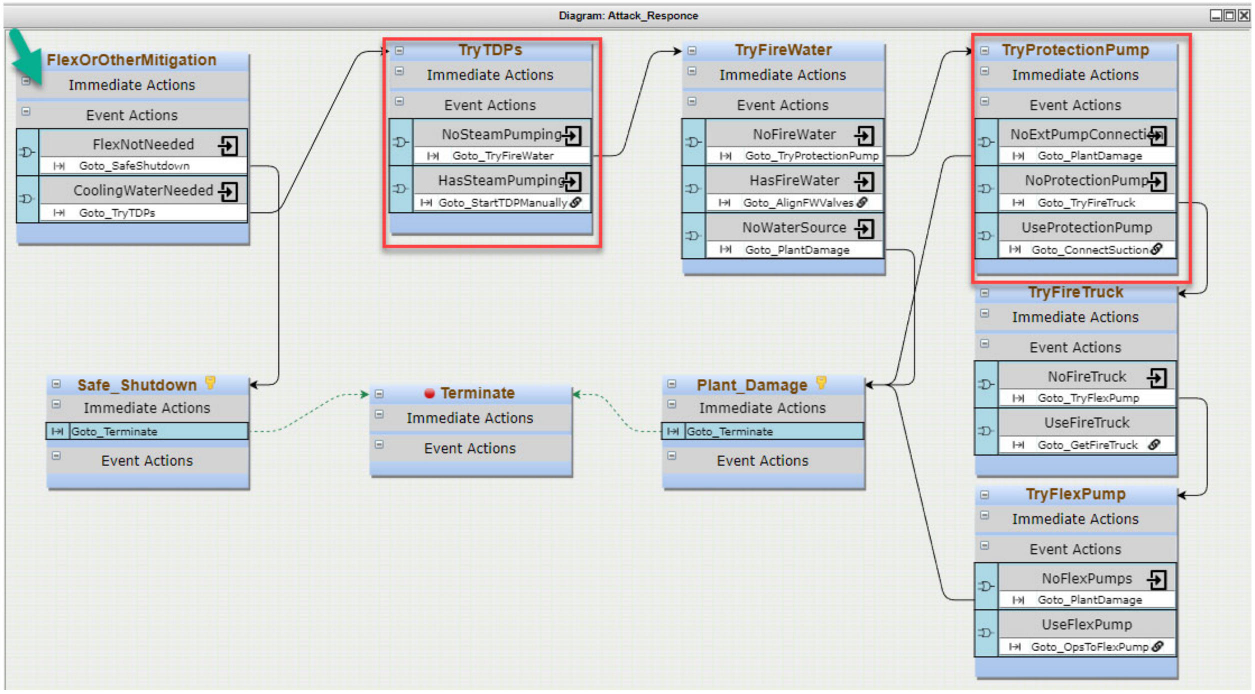


Figure 5. The Attack_Response diagram determines what mitigation options are available; for this pilot, only manual operation of turbine driven pumps and use of a protection pump where included (highlighted in red).

2.3. MAAP Model

A thermal-hydraulic Modular Accident Analysis Program (MAAP) model was used to determine if and when core damage occurs. This model was provided by the facility, and parameters were included to set times for the loss of the various cooling options, such as motor-driven pumps and TDPs, and then a parameter for when the security pump starts cooling. It is postulated that the plant operator fills the SG during an attack to provide an adequate cooling margin before backup injection from the protection pump is needed. The MAAP model is adjusted to include the start and end time for the SG-filling activity. This input file is modified by EMRALD to set the times to when they occur in the simulation.

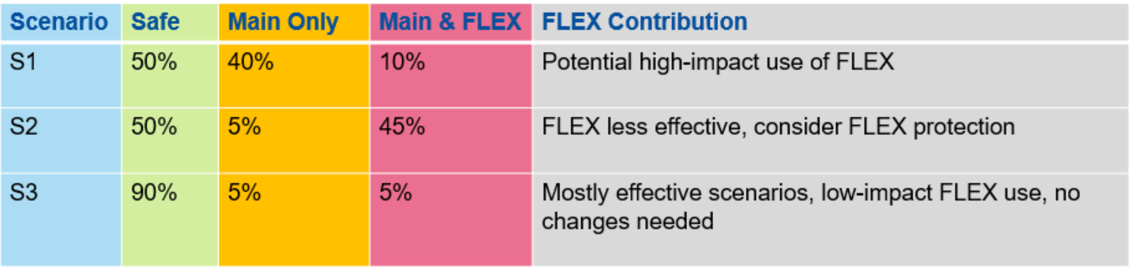
2.4. Initial Scenario Evaluation

The first step in performing this type of security risk evaluation is to review the existing attack scenarios and determine which scenarios include damage to equipment that could reasonably be mitigated using the standby equipment or other operator actions. For the example evaluation, the collaborating site provided experts from security, operations, PRA, and FLEX system engineers. The team reviewed existing security scenarios by targets, the difficulty to protect against, and after-attack mitigation options. The review determined that water injection into the SG from a standby pump would provide cooling to the core and would mitigate several scenarios. There were several scenarios where a generator could be beneficial, but the pump would also work as a mitigation. Initially, the use of an external FLEX pump was evaluated; this was changed to a protection pump inside the PA after reviewing initial results as discussed later in Section 3.

Before performing the post-reduction process, an initial analysis was done to determine whether the FLEX pump and SG-filling operator procedures could be effective as outlined in the MASS-DEF process. To do this, the targets in the FOF model were broken up into two groups, with the main targets in one group and the FLEX along with the hookups required for FLEX equipment in another, to evaluate if the adversaries were able to damage just the main targets or both the main targets and FLEX targets in the attack scenarios. This is done using an exaggerated strategy as specified in section 2.2.1 of “Guidance Documents for Using Dynamic Force-on-Force Tools” [8], in order to test the defense-in-depth security postures more fully.

Table 1 shows a hypothetical example of a few scenarios. The original model column shows the percentage of safe versus main targets hit, before adding any defense-in-depth modifications. Safe indicates at what percentage the guards stopped the adversaries from hitting all of the items in a target set. Main only indicates if they only hit the initial target set items. The Main and FLEX column indicates the percentage of time both Main and FLEX targets were hit, and so no after attack mitigation is possible. The ideal case for the maximum FLEX benefit would be for the main-only column to be as close to 100% as possible with a very low main-and-FLEX percentage, such as in row S1. In Table 1, S2 is a significant contributor to a physical security risk, but FLEX is also hit most of the time; so to be effective, some sort of protection or modification needs to be added to the FLEX connections. S3 is still a well-protected event with the exaggerated strategy, so FLEX may not be useful until guard reduction is applied. Scenarios like S3 need to be included to ensure we are not reducing effectiveness when going through the guard reduction process as described in Section 2.5.

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



Scenario	Safe	Main Only	Main & FLEX	FLEX Contribution
S1	50%	40%	10%	Potential high-impact use of FLEX
S2	50%	5%	45%	FLEX less effective, consider FLEX protection
S3	90%	5%	5%	Mostly effective scenarios, low-impact FLEX use, no changes needed

2.5. Guard Post-Reduction

The increased margin achieved by implementing standby equipment and other operator procedures in the security plan could allow for the removal and shifting of existing guard posts. Some scenarios require additional guards to protect against specific targets, by adding the FLEX targets for those scenarios. Existing guards can now protect against those scenarios, given that FLEX options can recover from primary target sabotage. The iterative method shown in Figure 6 and outlined in the MASS-DEF process [1] was used to optimize posts while maintaining the security effectiveness at an equivalent level.

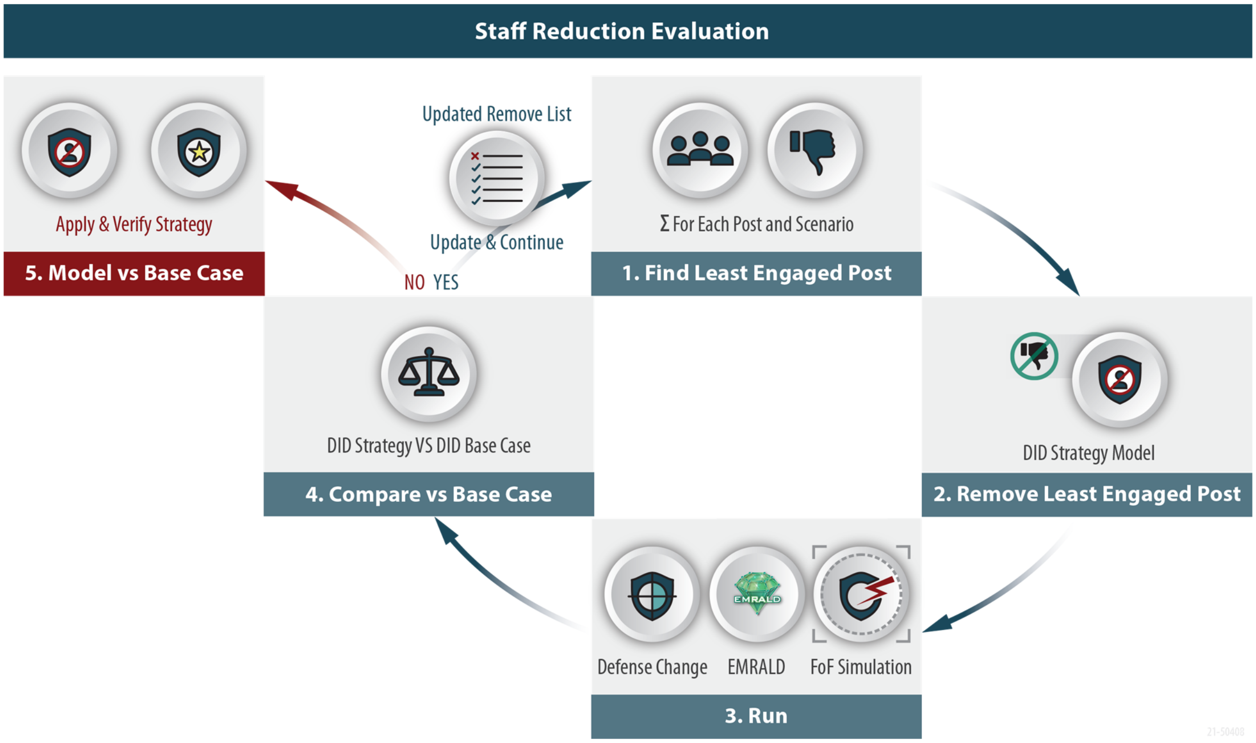


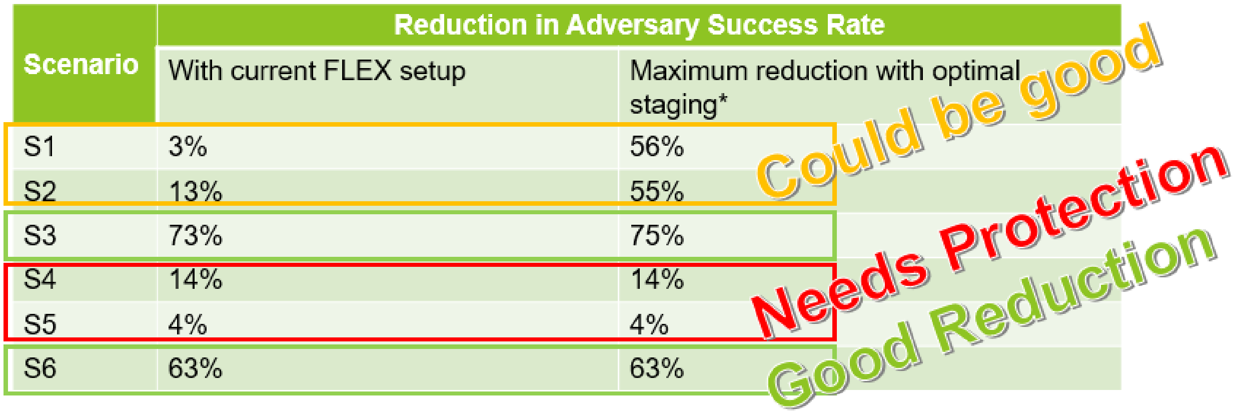
Figure 6. Guard post-reduction method process to maintain protection equivalency.

For this pilot analysis, the “Simajin/Vanguard Lethal Force Summary” report generated by the analysis was used to identify posts that contributed less to the baseline analysis and, as such, are candidates for removal in the reduction analysis. The candidate posts were removed for the defense-in-depth analysis in an iterative fashion, and as each was removed, the FOF simulations were executed, and the EMRALD analysis was applied to determine the adjusted probability of neutralization. The neutralization values between the original and subsequent reduction simulations were compared to verify that system effectiveness remained equivalent. After the candidate reductions were identified, the baseline scenarios were re-executed with the reduced defense to verify that there was no impact to overall system effectiveness.

3. RESULTS AND DISCUSSIONS

The generic PWR model was modified for plant-specific timing and an estimation for filling the SG. This model was run with the initial scenario results from Simajin/Vanguard. The detailed results of the simulations are categorized as safeguards information under 10 CFR part 73, and are therefore not published in this paper. However generically, Table 2 shows the reduction in attack success scenarios from the initial runs. This shows that two scenarios, S3 and S6, significantly benefited by the FLEX pump and operator actions. FLEX could also help scenarios S1 and S2 if the pump would have arrived sooner or was staged inside the PA. FLEX did not significantly help scenarios S4 and S5 because the secondary targets were often hit along with the main targets and would probably not help with post-reduction.

Table 2. Initial scenario evaluation when including FLEX pump and operator procedures.



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

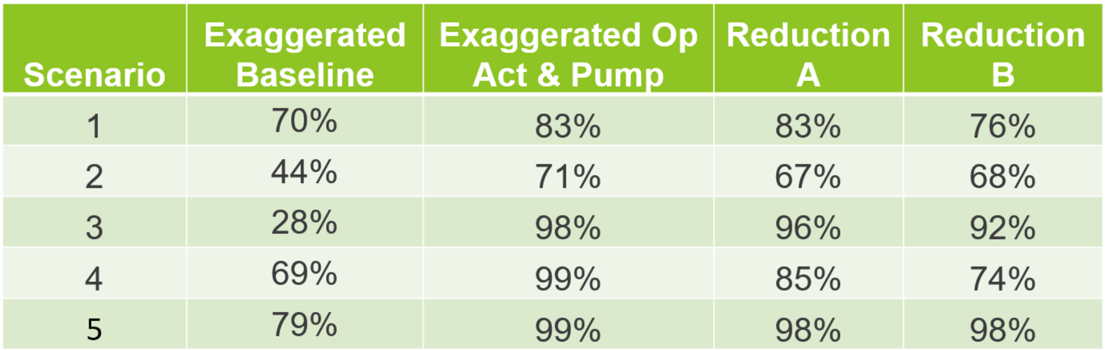
Could be good
Needs Protection
Good Reduction

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

Given that only two scenarios benefited, the idea of staging a FLEX pump was considered. While this would help these scenarios, putting a FLEX pump inside the PA would require considerable expense, and the use of FLEX equipment from outside the PA could cause other regulatory issues. To overcome this expense and regulatory issue, the idea of a security pump with the same specifications as a FLEX pump but without needing extensive severe weather protection was used. A plant modification to add an additional FLEX connection in a security strategic location was also planned.

After staging the security pump, adding the additional flex connection, and adding some security modifications currently planned the analysis was ran again. Exaggerated scenarios were used on the new model for the baseline. Then the additions of the operator actions and security pump inside the PA were added. Column 2&3 in Table 3 shows the large improvement made from these additions. Next, the guard reduction process was used where one or more guards were removed and others repositioned. The first set of changes shown in the “Reduction A” shows a slight reduction but still way above the exaggerated baseline. This means a further reduction can be done, again a set of changes was determined for “Reduction B” and as shown in table 3, it also was still above the exaggerated baseline. Given that there is still margin between “Reduction B” and the baseline, a third reduction, “Reduction C”, is being evaluated. This evaluation is still not complete at the time of this paper. If “Reduction C” is still above the baseline then it will be used for the final verification, if not, then “Reduction B” will be used.

Table 3. Defense success for the baseline, added operator actions with mitigation, and reduction steps, for exaggerated scenarios.



Scenario	Exaggerated Baseline	Exaggerated Op Act & Pump	Reduction A	Reduction B
1	70%	83%	83%	76%
2	44%	71%	67%	68%
3	28%	98%	96%	92%
4	69%	99%	85%	74%
5	79%	99%	98%	98%

The final simulation verification as described in the Staff Reduction Process and shown in **Figure 6**, will use the final reduction model with the normal, non-exaggerated scenarios, to do a final verification comparison with the original plant model. Reduction B achieved a 20% reduction in the engagement force and so at a minimum this work shows the use of operator actions and a security mitigation pump can provide a significant decrease in security force needed at a facility while maintaining current protection levels.

ACKNOWLEDGMENTS

This manuscript has been authored by Battelle Energy Alliance, LLC under Contract No. DE-AC07-05ID14517 with the U.S. Department of Energy. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for U.S. Government purposes.

REFERENCES

1. Christian, R., V. Yadav, S. R. Prescott, and S. W. St. Germain, 2022, “A Dynamic Risk Framework for the Physical Security of Nuclear Power Plants,” *Nuclear Science and Engineering*, https://doi.org/10.1080/00295639.2022.2112899.
2. U.S. Nuclear Regulatory Commission, title 10, part 50, section 54, “Conditions of licenses,” https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0054.html.
3. U.S. Nuclear Regulatory Commission, title 10, part 73, “Physical Protection of Plants and Materials,” https://www.nrc.gov/reading-rm/doc-collections/cfr/part073.
4. U.S. Federal Register, 85 FR 76625, “Physical Protection Programs at Nuclear Power Reactors Safeguards Information,” https://www.federalregister.gov/documents/2020/11/30/2020-26273/physical-protection-programs-at-nuclear-power-reactors-safeguards-information.
5. Idaho National Laboratory, n.d., “EMRALD,” https://emrald.inl.gov/SitePages/Overview.aspx.
6. RhinoCorps Ltd. Co., n.d., Accessed on April 20, 2023, https://www.rhinocorps.com/
7. ARES Security, 2022, “AVERT Suite,” Accessed November 14, 2022, https://aressecuritycorp.com/software/avert-suite.
8. Christian, R. S. R. Prescott, C. P. Chwasz, V. Yadav, and S. W. St. Germain, 2021, "Guidance Document for Using Dynamic Force-on-Force Tools," INL/EXT-21-64214, Idaho National Laboratory, https://lwrs.inl.gov/Physical%20Security/Guidance_Using_Dynamic_FoF_Tools.pdf.