INL/CON-23-71500-Revision-0

Technical and Regulatory Aspects of Integrating Safety and Security at Nuclear Power Plants

July 2023

Changing the World's Energy Future

Robby Christian, Steven R Prescott, Shawn W St Germain, Vaibhav Yadav, Christopher Paul Chwasz

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/CON-23-71500-Revision-0

Technical and Regulatory Aspects of Integrating Safety and Security at Nuclear Power Plants

Robby Christian, Steven R Prescott, Shawn W St Germain, Vaibhav Yadav, Christopher Paul Chwasz

July 2023

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

INL/CON-23-71500

Technical and Regulatory Aspects of Integrating Safety and Security at Nuclear Power Plants

Robby Christian[1], Steven R. Prescott[1], Vaibhav Yadav[1], Shawn W. St Germain[1], Christopher P. Chwasz[1]

[1]Idaho National Laboratory, Idaho Falls, ID

[leave space for DOI, which will be inserted by ANS]

ABSTRACT

This paper provides an overview of lessons learned in applying a dynamic computational framework that links results from a commercially available force-on-force (FOF) simulation tool, a commercially available thermal-hydraulic tool, and the Event Modeling Risk Assessment using Linked Diagrams (EMRALD) for an operating commercial nuclear power plant. This process of including plant procedures and multiple analysis results is being called Modeling and Analysis for Safety Security using Dynamic EMRALD Framework. It describes how a user could integrate their plant-specific FOF models with safety mitigation actions in EMRALD and with thermal-hydraulic tools, such as the Modular Accident Analysis Program.

The work performed in this paper is based on a generic EMRALD model with actual plant data used for the analysis. However, we are only presenting the generic model and general results of the analysis for dissemination. No plant's sensitive information is in this paper. The discussion shows examples of insights from our proposed methodology.

Keywords: EMRALD, physical security, safety

1. INTRODUCTION

1.1. Background

The Department of Energy has established the Light Water Reactor Sustainability Program to support the continued operation of nuclear power plants in the United States amidst 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. Modeling and simulation are used to evaluate the margin inherent in many security postures and to identify ways to maintain overall security effectiveness while lowering costs. Two areas we identified for evaluation are taking credit for the diverse and flexible mitigation capability (FLEX) equipment and actions taken by operators to minimize the possibility of reactor damage during an attack scenario. In other words, crediting existing safety measures to prevent radiological release following a sabotage attack.

1.2. Regulatory Aspects

The Nuclear Regulatory Commission (NRC) and industry approach to maintaining effective security at a plant includes various security programs—each with its own individual objectives; when combined, these programs provide a holistic approach to maintaining the effective security of the plant. The NRC regulations, 10 CFR 73.55(d)(1), state, "The licensee shall establish and maintain a security organization that is designed, staffed, trained, qualified, and equipped to implement the physical protection program in accordance with the requirements of this section" [1]. 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 [2]. The plant's response force includes the minimum number of armed responders, as required in 10 CFR 73, and security officers tasked with assigned duties, such as stationary observation and 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 value for facilities to accurately evaluate time and mitigation options.

2. METHODOLOGY

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

The criterion used for determining defense success or failure against an attack is typically if the adversaries reach the attack targets. However, this is a conservative assumption, because realistically there are extra steps and elapsed time before they can induce a significant radiological release. These steps and time may also be affected by preventive actions from the plant operator, for example whether the reactor was shut down prior to the attack and at what time relative to the sabotage time of attack targets. Such preventive actions may alter whether and when the core is damaged following a successful sabotage. A plant thermal hydraulics model, such as Modular Accident Analysis Program (MAAP), could be used to determine the timing and outcome of the attack scenario.

2.1. Modeling Diverse and Flexible Mitigation Capability and Mitigation Tasks

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 for dynamic safety and physical security evaluations. The INL team developed a generic EMRALD model that imports force-on-force (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 or AVERT. This generic model captures the well-known behavior of pressurized-water reactor (PWR) nuclear power plants to determine if FLEX equipment could prevent core damage. With the generic nature of the model, the results would not be safeguards information. The generic model incorporates basic PWR safety elements, such as the control room, diesel generators (DGs), motor-driven pumps, turbine-driven pumps, 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.

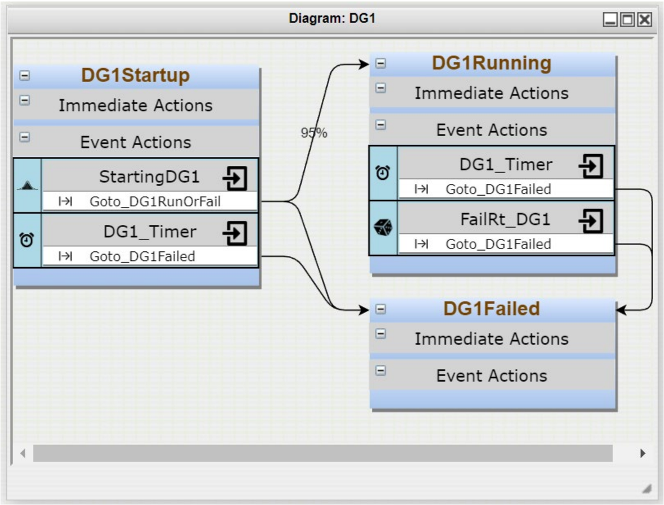
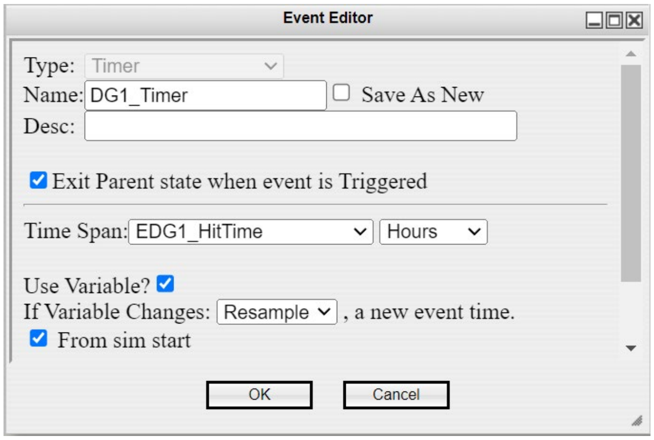


Figure 1. DG operational diagram.

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) provides the time data for when the generators are sabotaged. This data is recorded in EMRALD variable EDG1_HitTime and EDG2_HitTime for the first and second generator, respectively. The DG1_Timer event shown in Figure 3 uses this timing variable to switch the generator state from DG1Running to DG1Failed. With this modeling approach, the generators may run for some time before they are sabotaged. This dynamic equipment availability information can be fed into a reactor safety analysis code to evaluate the resulting reactor state.


Event Editor

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

☑ Exit Parent state when event is Triggered

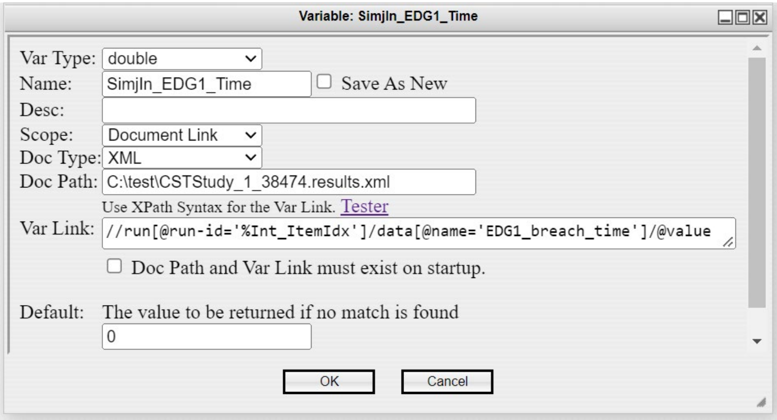
Time Span: EDG1_HitTime Hours

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 running an external FOF simulation and extracting the output data, either through a close coupling while the external simulation is still running or after it is completed. After reading the output file, the AttackDetected event is activated after a certain delay time governed by the FOF output data. The event triggers the FoF_Engagement state, which waits for the specified amount of time for the attack to complete, again by using the time data from FOF. After the attack ends, a team of armed responder is dispatched to sweep the plant and ensure it is secure for safety personnel to initiate FLEX mitigation actions if needed. This procedure may differ for each plant. For example, a plant with predeployed FLEX equipment in a secured room may choose to dispatch FLEX operators early upon detecting an attack.

The actions to extract select FOF data rely on variables coupled with the extensible markup language (XML) output file of the FOF software. Figure 3 shows a sample of this variable for an emergency diesel generator's (EDG's) sabotage time. The Doc Path field locates 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.



Variable: SimjIn_EDG1_Time

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

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

2.2. A Generic Model for 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.

The generic model allows for multiple procedures to be added once an attack is detected. This is done by creating a new diagram in EMRALD, modeling that procedure, and then adding a link to start that procedure in the "AttackDetected" event under the "AttackSetup" state in the "Initiate_Attack" diagram, as shown on the left side of Figure 4. For this pilot, the pilot facility wanted to explore the option of filling the steam generators, as long as filling equipment was available, up to 80%. The filling procedure would begin as soon as an attack is detected.

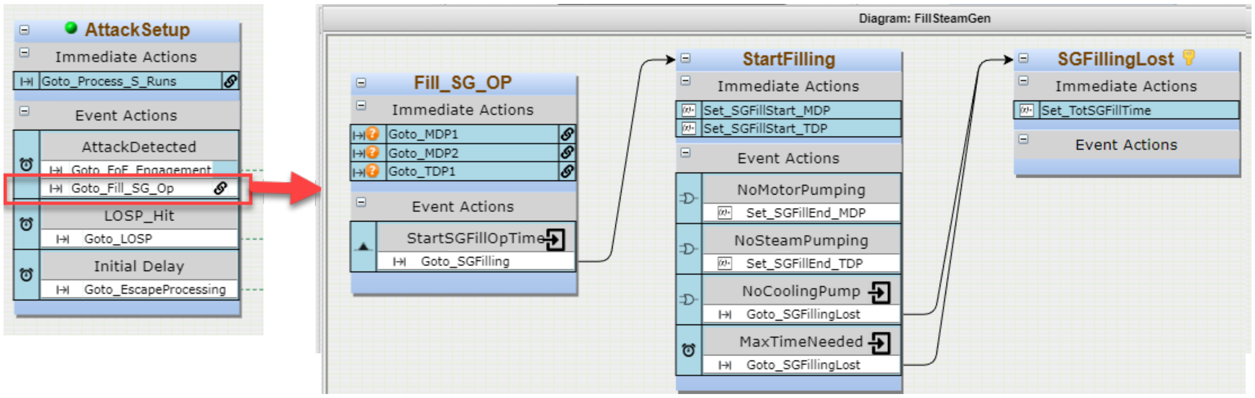


Figure 4. (Left) Attack detection triggering evaluation of the EMRALD diagram (Right) of the procedure to fill the steam generator after detecting an attack.

Filling the steam generators provides a larger inventory of cooling water if an attack is successful in disabling other forms of heat removal. There are three states in the fill procedure: Fill_SG_OP, StartFilling, and SGFillingLost. In the first state, Fill_SG_OP, the fill pumps are verified available, then the time it takes the operator to verify the attack alarm and start the filling process is represented by the distribution event StartSGFillOpTime. The procedure used an initial normal time distribution value of 30 seconds with a standard deviation of 5 seconds for the StartSGFillOpTime event. Further research will determine accurate times for this procedure to get more reliable results. Once this time is up, the simulation moves to the StartFilling state in the diagram. Here, the system waits until either all the filling pumps have failed or the maximum time needed to fill the steam generator has expired, before moving to the third state in the diagram (i.e., the SGFillingLost state).

Meanwhile, the post-attack mitigation actions are modeled as shown in Figure 5. The current work utilizes the FLEX strategy to prevent core damage following a sabotage attack. First, the model evaluates if FLEX is needed then starts the simulation piece for the FLEX procedures. An example mitigation action is provided when a loss-of-offsite-power event happens. It activates the DGs and their cooling system. If backup power from generators is unavailable, the plant enters the station blackout state, and the Need_DC_Power event is triggered. If the design basis safety system can mitigate the sabotage, the FlexNotNeeded event is active and brings the plant to the Safe_Shutdown state. Otherwise, the FLEX equipment needed is determined by a logic tree evaluation, either FLEX generator or pump. For the pilot scenario, we determined that only the FLEX pump was needed for their scenarios.

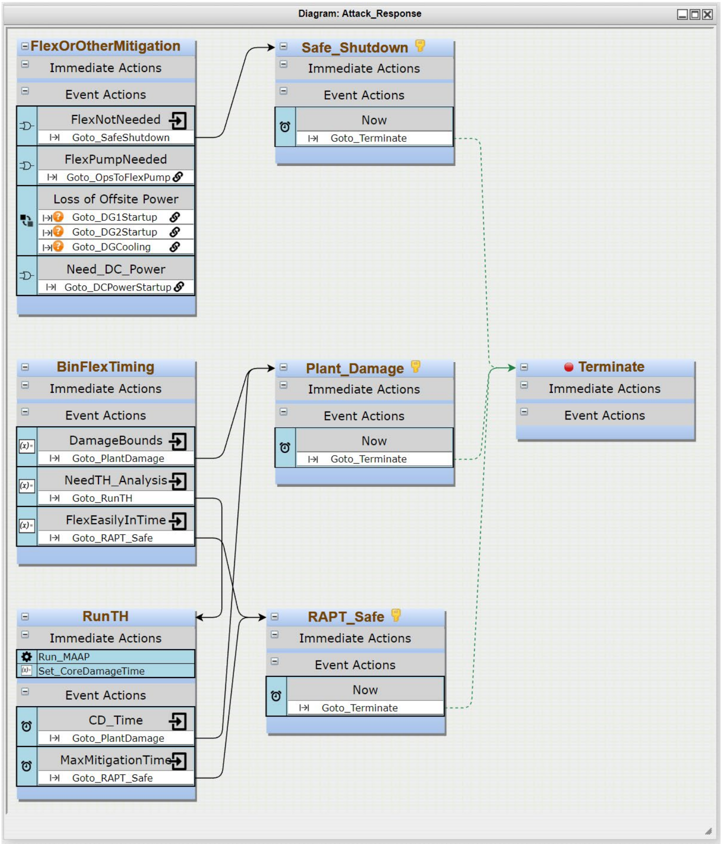
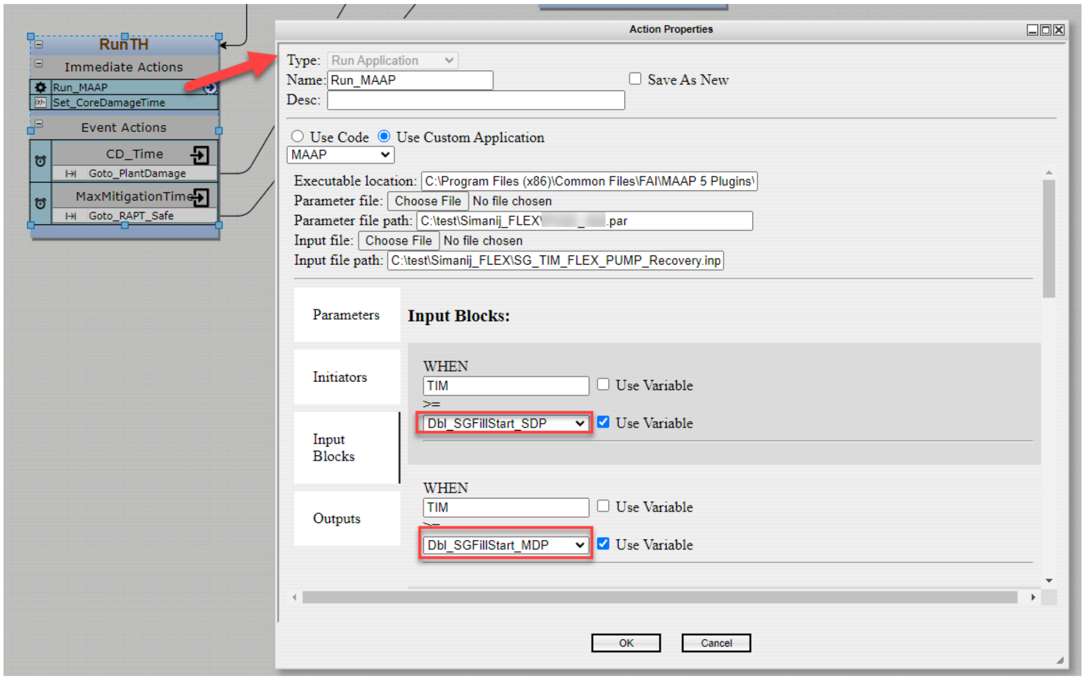


Figure 5. The Attack_Response diagram evaluates and starts FLEX, evaluates procedure times, and runs thermal hydraulics to determine plant damage.

2.3. MAAP Model

A thermal-hydraulic MAAP model is used to determine if and when core damage occurs. This model needs to have parameters to set times for the loss of the various cooling options and include features for FLEX cooling along with a set time parameter. It is postulated that the plant operator fills the steam generator (SG) during an attack to provide an adequate cooling margin before backup FLEX injection is needed. The MAAP model is then adjusted to include the start and end time for the SG filling activity. This input file is modified by EMRALD to set the times according to the times they occur in the simulation. The EMRALD interface to modify these MAAP parameters is shown in Figure 6.



Action Properties

Type: Run Application
Name: Run_MAAP   □ Save As New
Desc:

○ Use Code ● Use Custom Application
MAAP

Executable location: C:\Program Files (x86)\Common Files\FAI\MAAP 5 Plugins\
Parameter file: Choose File No file chosen
Parameter file path: C:\test\Simanij_FLEX\[redacted]_[redacted].par
Input file: Choose File No file chosen
Input file path: C:\test\Simanij_FLEX\SG_TIM_FLEX_PUMP_Recovery.inp

Input Blocks:

WHEN
TIM □ Use Variable
>=
Dbl_SGFillStart_SDP ☑ Use Variable

WHEN
TIM □ Use Variable
>=
Dbl_SGFillStart_MDP ☑ Use Variable

Figure 6. EMRALD form to set up MAAP execution and get results.

A nuclear power plant collaborated with INL in this research. The results discussed in this paper are obscured such as that they do not reveal sensitive information on the plant security posture. The first step in performing this type of security risk evaluation is to review the existing attack scenarios and determine which scenarios include damage to equipment that could reasonably be mitigated using FLEX equipment or other operator actions. For the example evaluation, the collaborating site provided experts from security, operations, PRA, and FLEX system engineers. The team reviewed existing security scenarios by target, difficulty to protect against, and after attack mitigation options. The review determined that fire water injection into the SG or a FLEX pump providing cooling to the SG could be used to mitigate several scenarios. There were several scenarios where a FLEX generator could be beneficial, but the pump would also work as a mitigation. The FLEX pump was also slightly faster to transfer and hook up, so only the FLEX pump was used in the analysis.

2.4. Sensitivity Analysis

Before connecting EMRALD to the FOF results, an initial analysis determined if the FLEX and other operator procedures could be effective by putting the main targets in one group and the FLEX in 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.

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

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

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

2.5. Guard Optimization

The increased margin achieved by implementing FLEX and other operator procedures in the security plan could allow for the removal and shifting of existing guard posts. Some scenarios require additional guards to protect against specific targets, by adding the FLEX targets for those scenarios, existing guards can now protect against those scenarios, given that FLEX options can recover from primary target sabotage. The iterative method shown in Figure 7 and outlined in Reference [6] is being used to optimize posts while maintaining the security effectiveness at an equivalent level.

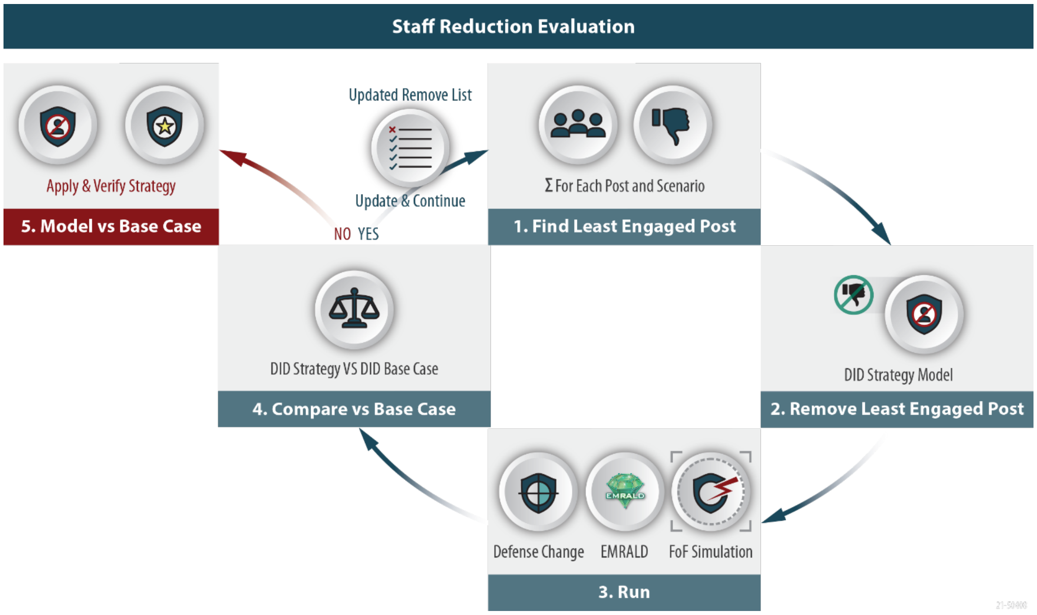


Figure 7. Guard post-reduction method process to maintain protection equivalency.

3. RESULTS AND DISCUSSIONS

The detailed results of the simulations are categorized as safeguards information and are therefore not published in this paper. However, there are general observations we can discuss here. We successfully modified and applied the generic PWR EMRALD model to this example security risk assessment evaluation. It successfully pulled in data from the external FOF tool, simulated plant FLEX procedures, and ran the MAAP thermal-hydraulic code to determine scenario outcomes.

Six scenarios were evaluated for the use of a FLEX pump for mitigation after an attack. Two scenarios, S3 and S6, had a high reduction of adversary success. Two others, S1 and S2, were not very successful because there was usually not enough time to get the pump and set it up in time. They could be successful if a pump was already staged inside the protected area. The final two scenarios, S4 and S5, did not benefit because FLEX connection points were too easy to sabotage along with the other existing targets. For scenarios S4 and S5, a plant modification would be needed to better protect FLEX equipment and connections.

Table 2. Scenario mitigation success percentage using FLEX equipment.

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%

*With reduced time to obtain cooling (i.e., closer FLEX, pre-staged, and protected).

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

- FLEX equipment stored outside of the protected area may not be able to be credited in a target set analysis. Plant-specific considerations will dictate which option is more cost effective, including:
  - Purchase another pump, similar to the FLEX pump, as a security response pump that would be stored inside the protected area, in a protected location, so the operations procedures, maintenance, and deployment would be similar if not identical to the existing FLEX equipment
  - Pre-stage an existing FLEX pump/equipment inside the protected area
- Ensure there is enough time to deploy FLEX equipment, through either or both of the following:
  - Pre-stage FLEX equipment somewhere easily protected through physical security measures
  - Add procedures to fill steam generators to a higher level when an attack is detected
- Ensure the sufficient physical protection of FLEX equipment and connections
  - Connections or pre-staged equipment should be strategically located for effective protection by plant security forces and separated physically from other target set equipment locations
  - Connections or pre-staged equipment should have access delay features, such as fencing.

In conclusion, we obtained reasonable results and identified several valuable insights about the potential effectiveness of crediting FLEX equipment in security scenarios. The lessons learned from this study will be used to work with industry to create a guidance document outlining a detailed process to perform this type of analysis.

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 United States Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for U.S. Government purposes.

REFERENCES

1. U.S. Nuclear Regulatory Commission, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage," Regulations (NRC, 10 CFR), Part Index, https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0055.html (n.d.).
2. U.S. Nuclear Regulatory Commission, "Emergency Preparedness in Response to Terrorism," About Emergency Preparedness, https://www.nrc.gov/about-nrc/emerg-preparedness/about-emerg-preparedness/response-terrorism.html#one (2020).
3. U.S. Nuclear Regulatory Commission, "PART 73—Physical Protection of Plants and Materials," Regulations (NRC, 10 CFR), https://www.nrc.gov/reading-rm/doc-collections/cfr/part073 (2021).
4. U.S. Federal Register, "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 (2020).
5. Idaho National Laboratory, "EMRALD," https://emrald.inl.gov/SitePages/Overview.aspx (n.d.).
6. R. Christian, V. Yadav, S. R. Prescott, and S. W. St. Germain, "A Dynamic Risk Framework for the Physical Security of Nuclear Power Plants," *Nuclear Science and Engineering*. https://doi.org/10.1080/00295639.2022.2112899 (2022).