INL/CON-21-62280-Revision-0

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

April 2021

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

Changing the World's Energy Future

Idaho National Laboratory

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

INL/CON-21-62280-Revision-0

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

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

April 2021

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

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

Robby Christian, Vaibhav Yadav, Stephen Prescott, and Shawn St. Germain
Idaho National Laboratory
1955 N. Fremont Ave., Idaho Falls, ID
robby.christian@inl.gov; vaibhav.yadav@inl.gov; steven.prescott@inl.gov; shawn.stgermain@inl.gov

ABSTRACT

This paper describes ongoing work within the Light Water Reactor Sustainability (LWRS) Program at Idaho National Laboratory (INL) to optimize security and cost of nuclear power plants (NPPs). It reviews the conservatisms in conventional physical security posture and regulations. It introduces the dynamic risk assessment tool developed at INL, Event Modeling Risk Assessment using Linked Diagrams (EMRALD). The dynamic assessment methodology leverages EMRALD to process results of force-on-force (FOF) simulations and crediting safety mitigation actions from probabilistic risk assessment (PRA) models as well as diverse and flexible coping strategies (FLEX) mitigation strategies. Timing information from these simulations are compared against the available time to perform mitigations obtained from Reactor Excursion and Leak Analysis Program (RELAP5) simulations.

To illustrate the methodology, a station blackout (SBO) attack scenario was modeled in commercially available FOF simulation tools. The simulation results provide valuable insights into possible attack outcomes and as the probabilistic risk of a core damage event given these outcomes. Safety mitigation procedures were modeled in EMRALD, and were dependent on the attack outcomes by considering human operator uncertainties. RELAP5 simulations incorporating human and hardware uncertainties were performed to estimate the distribution of time-to-core damage.

The results demonstrate that, even in the extreme case of a successful adversarial attack, plant mitigation strategies provide significantly high-likelihood of preventing radiological release. The proposed 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.

Key Words: Physical security, FLEX, EMRALD

1 INTRODUCTION

The increased penetration of natural gas and renewables in the deregulated energy market in the U.S. has created financial challenges for baseload power plants including nuclear power plants (NPPs). Utilities are working hard to modernize plant operations to lower the cost of generating electricity with NPPs. The Department of Energy established the Light Water Reactor Sustainability (LWRS) Program with the mission to support the current fleet of NPPs with research to facilitate lowered Operating and Maintenance (O&M) costs. Due to the use of nuclear materials, NPPs have an additional cost burden in protecting fuel against theft or sabotage. The overall O&M cost to protect NPPs accounts for approximately 7% of the total cost of power generation with labor accounting for half of this cost [1]. In the current research, from interaction with utilities and other stakeholders, it was determined that physical security forces account for nearly 20% of the entire workforce at NPPs.

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 was identified as one area that holds the potential to optimize the security posture and reduce costs. This paper 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.

1.1 Operating and Maintenance Costs

Figure 1-1 shows the revenue gap in U.S. NPPs from a study in 2017 [2]. It shows that a large portion of the power plants have negative revenues. Although this revenue gap is caused mainly by the market's situation as the study suggested, there may be actions the power plants can do to reduce its severity. Data from the Electric Utility Cost Group (EUCG) presented by the Nuclear Energy Institute suggests that a significant percentage of NPP costs come from O&M, which also includes maintaining the physical security posture. Optimization of physical security may help the NPPs to sustain operation if compliance to the regulation is maintained.

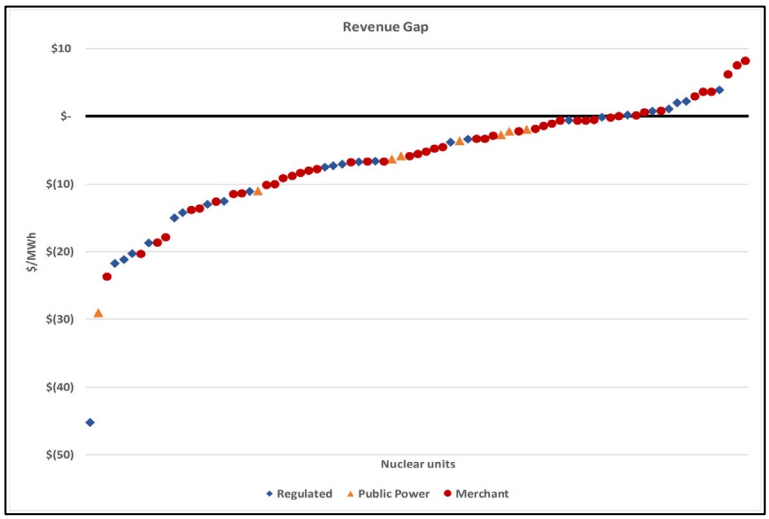


Figure 1-1. Revenue gap of NPPs in U.S. in 2017.

1.2 Regulation on the Physical Protection of Nuclear Power Plants

The requirements for physical protection on NPPs are given in 10 CFR 73.55 [3]. Clause (b)(1) of the regulation states the general performance objective and requirements of the physical protection system (i.e., "to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.") Furthermore, the regulation requires licensees to establish a physical protection program to achieve that objective. Specifically, this protection program "must be designed to prevent significant core damage and spent fuel sabotage" as required in clause (b)(3).

The regulation consists of mainly prescriptive requirements, given in clause (b) through (q). Several examples of these prescribed requirements are as follows:

- Clause (k)(5)(ii) requires licensees to provide a minimum of ten armed responders, who shall be available at all times inside the protected area
- Clause (n)(v)(2) requires licensees to test intrusion alarm at least every 7 days

- Clause (b)(6) requires licensees to demonstrate the effectiveness of the armed responders and armed security officers following specific requirements set out in Appendix B of the regulation.

These prescribed clauses do not provide much room to optimize the physical protection system with respect to the security performance and costs. For example, if the licensee wants to utilize an advanced intrusion detection system (IDS) with automatic testing and online monitoring capabilities, such that a manual test every 7 days can be relaxed or eliminated, it would be considered insufficient to meet the regulation. Fortunately, there is an alternative measure in clause (r) of the regulation, which allows a licensee to provide a measure for protection rather than the prescribed measures, given that the alternative measure meets the same performance objective specified in clause (b). However, this alternative measure has not been widely pursued. It may be caused by the difficulties in analyzing system performance with the existing tools to account for equipment changes and incorporation of plant safety measures. Optimization of physical security systems may be done through this performance-based clause by systematically measuring the protection's effectiveness.

2 METHODOLOGY

2.1 Design Evaluation and Process Outline Methodology

The Design Evaluation and Process Outline (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 evaluation step is described in this section.

Given a specific facility, an attack pathway can be evaluated by simplifying the facility in an adversary sequence diagram (ASD) model. Figure 2-1 illustrates an ASD of a hypothetical facility. It lays out the areas within the facility, such as offsite area, facility campus area, and reactor complex area, to the hardened room in which a radioactive material is stored, as well as the barriers separating the areas, such as facility fence, facility gate, doors, walls, and roofs. Detection probability (P_D) and traversal time (T) through each area/barrier are entered in the ASD. These values are evaluated independently for each area/barrier and are typically conservative. The fastest adversary path can be created by summing the ASD blocks which have the least T in, while the most stealth path is created by traversing through the blocks with the least P_D.

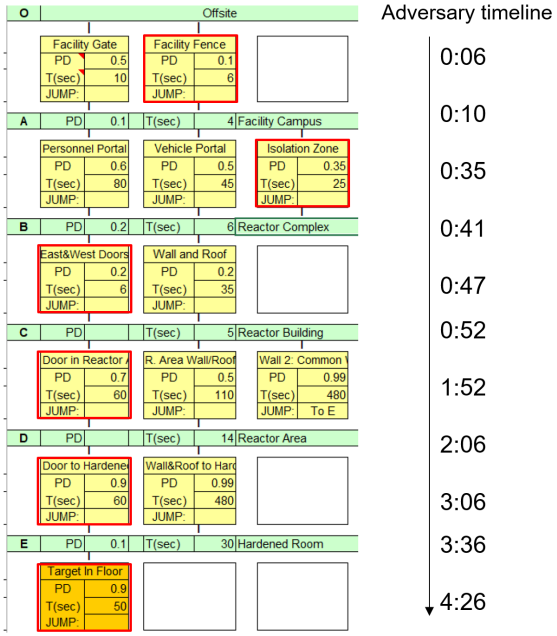


Figure 2-1. Adversary Sequence Diagram (ASD).

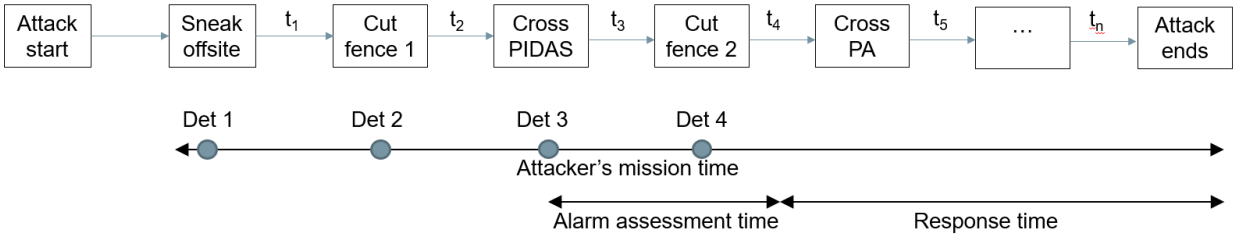


Figure 2-2. Attack and response timeline.

The attack path is used to formulate the attack timeline as illustrated in Figure 2-2. The times to perform actions are constant. In addition, the guards' response time and alarm assessment time are shown in the figure. With such response time, Detector number 3 (Det 3) is designated as the critical detection point (CDP), beyond which the intrusion alarm system is not credited in the PPS because it would have been too late to intercept the adversaries in time. The cumulative probability for the PPS to intercept adversaries before they finished their attack is given by the probability of interruption P_I:

$$P_I = 1 - \prod_1^3 (1 - P_D)_i \quad (1)$$

In which Detector number 4 (Det 4) is excluded, despite it being in the system, because it is located beyond CDP. The PPS effectiveness is formulated as:

$$P_E = P_I \times P_N \quad (2)$$

Where P_N is the probability for the response force to neutralize the attackers.

Since it is simple and easy to use, this methodology has its advantages. However, it uses conservative assumptions such as simplification of uncertainties, statistical independence, and underestimation of the intrusion alarm system. This conservatism may result in a costly PPS design. Furthermore, it assumes that the security objective is defeated when the adversaries completed their task. NPPs are complex industrial systems employing redundant safety mechanisms to prevent accidents. There is an elapsed time before the nuclear core may be damaged after adversaries disable targeted components of the plant. Within this timeframe, there are mitigation actions that can be done to prevent the adverse effect of an attack, either by using the design basis safety systems or additional actions such as the FLEX strategy. In this paper, we analyze the feasibility of incorporating these safety actions to support the objective of physical security (i.e., prevention of core damage).

2.2 Proposed Dynamic Methodology

Figure 2-3 illustrates a possible, realistic look at the attack timeline. The center timeline represents the initial attack plan. When adversaries sneak into the offsite area, they may be seen by armed guards on patrol, in which case the adversaries may retreat and resume the attack another time, or they may open fire at the guards. The time distribution to cut the fence in the planned condition is $P(t_1)$; however, if the adversaries are under fire, this action may take a longer time as $P(t_2)$. If the adversaries are sufficiently slowed down, the response force may arrive while they were still in the perimeter intrusion detection and assessment system (PIDAS). When adversaries cut the fence, the cutter may break, and they may cancel the attack altogether, or they may climb the fence. Climbing the fence may increase the detection probability and alter the task completion time. Since the cutter has failed, they may likewise climb the inner fence instead of cutting it as planned.

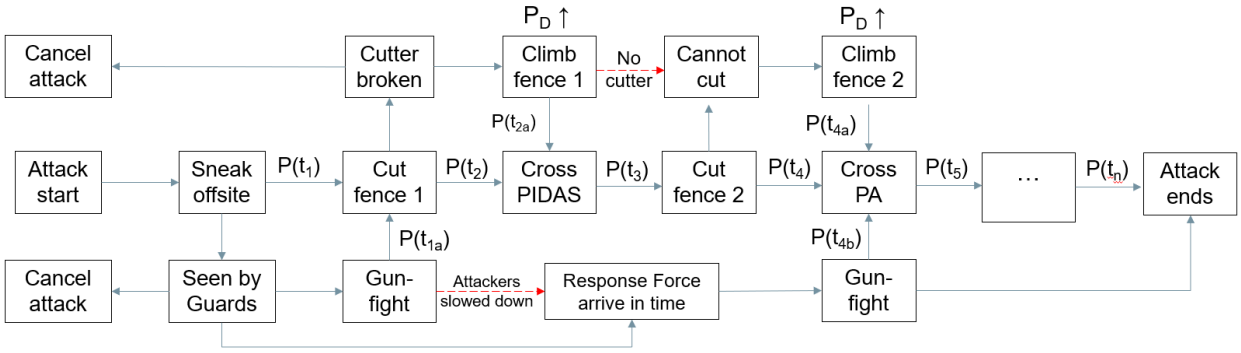


Figure 2-3. Possible variations of an attack plan.

The possible scenarios described above imply that despite the conservative assumptions on attackers' capabilities, there are various ways an attack plan can go wrong. Furthermore, the different ways a plan goes wrong may affect the next steps of attack or intervention actions. Therefore, there are dynamic dependencies among the steps. These dependencies mean that the mission time may not be constant. These are implications of introducing realism into the evaluation of PPS, which are different than the assumptions employed in the static methodology described in the previous section.

The PPS effectiveness in the dynamic methodology is conceptually formulated as:

$$P_E = P_D|A \times P_t|D \times P_N|t \tag{3}$$

Where $P_D|A$ is the probability of detection which is dependent upon the adversary's action, $P_t|D$ is the probability of timely interception which depends on the intrusion detection event, and $P_N|t$ is the probability of neutralization which depends on the time of response force's arrival. If the response force arrives early,

they may set up a defensive position which gives them an advantage to neutralize the incoming adversaries, as opposed to when they arrive later and are forced to engage while running. The dynamic dependencies in these variables are evaluated by simulating the uncertainties in the attack plan using the FOF simulation tool, AVERT [4].

2.3 Event Model Risk Assessment using Linked Diagrams

Event Modeling Risk Assessment using Linked Diagrams (EMRALD) is utilized primarily to model the uncertainties in safety actions to mitigate the outcomes of a sabotage attack described in the previous section. EMRALD is a dynamic probabilistic risk assessment (PRA) model that is based on a three-phased discrete event simulation. It is comprised of discrete states. In a state, there are multiple events, which are categorized into conditional events and time-based events. Conditional events occur when the specified conditions are fulfilled. Meanwhile, time-based events happen after a certain time has elapsed, which may be defined using probability distributions. When an event occurs, EMRALD executes certain actions modeled under that event. These actions may involve moving the simulation to another state, running an external simulation or a block of programming code, or modifying certain variables.

Diagrams in EMRALD are classified into several levels (i.e., overall plant level, system level, and component level). EMRALD can also model fault trees and trigger events based on the failure or success of the fault tree's top event. In this simulation, EMRALD is used together with AVERT, as well as plant thermal-hydraulics code, RELAP5-3D.

2.4 Integration of Force-on-Force Model with FLEX Strategy

Figure 2-4 shows the model used to integrate the FOF with FLEX [5]. The FOF model simulates the sabotage attack progression while EMRALD controls the overall simulation and models of the safety actions. When the first target element is sabotaged, operators begin to prepare FLEX equipment as modeled in EMRALD. When the attack ends, EMRALD retrieves the FOF data to assess the damage to the plant and the timing when a target is sabotaged. If all target sets are intact, the plant resumes normal operations after an emergency shutdown. If some equipment is compromised but the design basis safety systems are still functional, the event is mitigated using the design basis systems. If all target set elements are damaged, the FLEX mitigation strategy is used.

The time distribution to FLEX deployment from the EMRALD model is compared with the time distribution to core damage from the FOF and RELAP5 model. The competition between these two timings provides information on the likelihood of preventing core damage from the sabotage attack.

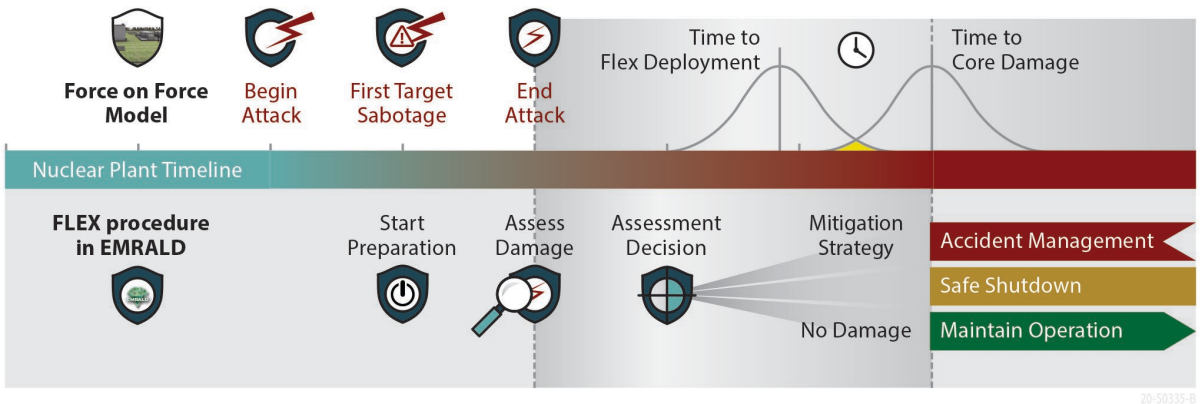
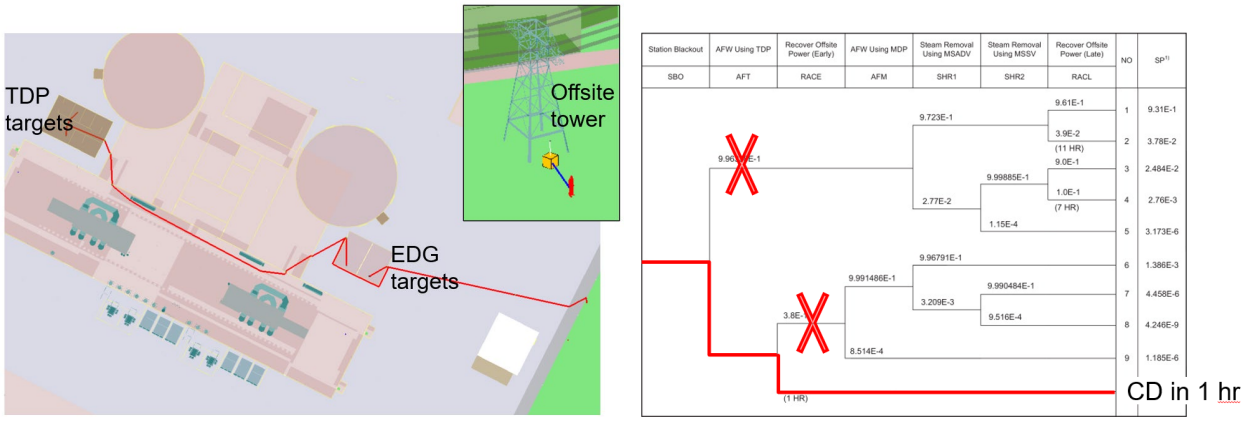


Figure 2-4. FOF-FLEX timeline model.

3 CASE STUDY

For a case study, a hypothetical pressurized water reactor (PWR) NPP was modeled in AVERT as shown in Figure 3-1(a). An adversary detonates the offsite electrical tower to create a loss-of-offsite-power event. In the meantime, four adversaries breached the reactor complex to sabotage the emergency diesel generators (EDGs) to create a station blackout (SBO) event and sabotage turbine driven pumps (TDPs) to create the core damage (CD) event. The event progression is shown in Figure 3-1(b). The static event tree estimates that CD happens in 1 hour.

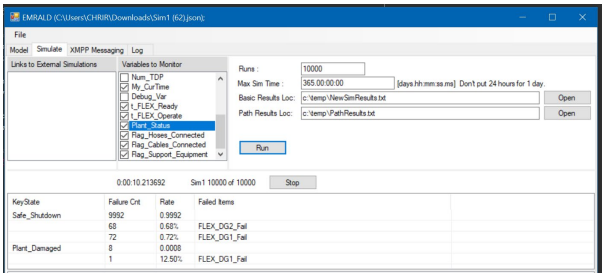


(a) Plant layout and target locations

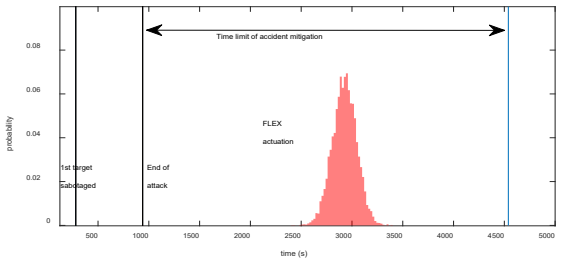
(b) Core damage event tree

Figure 3-1. Attack scenario.

The resulting timeline from a FOF simulation is shown in Figure 3-2. It shows discrete times when the first target is sabotaged, when the attack ends, and when the CD is supposed to happen within 1 hour. The EMRALD-FLEX model was run 10,000 times to produce a time distribution of FLEX actuation, which falls within the 1-hour limit. However, this time limit was designated with the assumption that the loss-of-offsite power, backup power, and passive safety injection happen at the same time. Meanwhile, in the attack scenario, there are periods of time between those events, to which the plant may respond differently, changing the CD timing. For that reason, analysis of uncertainties in the plant's thermal-hydraulic response were done in RELAP5.



(a) EMRALD solver window



(b) FoF-FLEX timeline

Figure 3-2. Results from one FOF attack scenario.

A series of thermal-hydraulic analysis was done in RELAP5 by including uncertainties from the operator action timing and component failures. These uncertainties are listed in Table 3-1 and Table 3-2.

Table 3-1. Uncertainties on operator's action timing.

Task	Average (s)	Std dev (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 Reactor Coolant System (RCS)	395.4	61.0
Preventing the over pressurization of main condensers	410.8	76.5
Restoring AC power	515.6	89.7

Table 3-2. Uncertainties on component failures.

Variable	Distribution
Number of 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)
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)

The results from these uncertainties are shown in Figure 3-3. It shows the timing distribution of FOF simulation results and distribution of FLEX actuation timing, which are less than the bins of the CD timing obtained from RELAP5 runs. Further analysis was done by varying the attack pathway in the FOF software while maintaining the target sets.

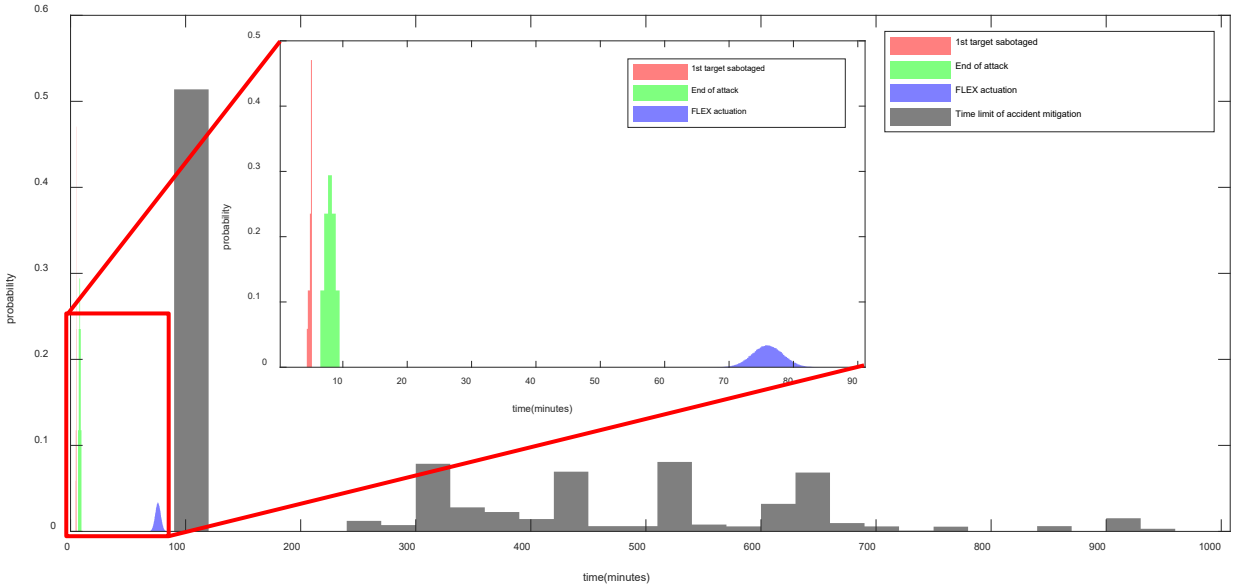


Figure 3-3. Timeline distribution considering uncertainties in CD timing.

There are eight possible outcomes of this sabotage attack listed in Table 3-3. The probability for each outcome is listed on the table which was obtained from FOF simulations. FLEX-EDG strategy was used for scenario number 7 to provide power to instrumentations and recharge steam valve batteries which regulate steam dump and turbine driven pump operations. Meanwhile FLEX extended loss of AC power (ELAP) strategy was used in scenario number 8 to provide power and inject feedwater to steam generators. Without a FLEX mitigation strategy, scenario number 8 always leads to CD. This scenario is the largest contributor to the conditional core damage probability (CCDP) value followed by scenario number 7. However, with FLEX strategies, the risk of these two scenarios were significantly reduced by a factor of 4. FLEX strategies reduce the plant's CCDP by an order of two.

Table 3-3. Summary of results.

No.	System availability			Mitigation strategy	Probability	CCDP without FLEX	CCDP with FLEX
	Offsite power	EDG	TDP				
1	Yes	Yes	Yes	N/A	0	0	0
2	Yes	Yes	No	Non-transient shutdown	0	0	0
3	Yes	No	Yes		0	0	0
4	Yes	No	No		0	0	0
5	No	Yes	Yes	LOOP ET	0.933	9.33E-4	9.33E-4
6	No	Yes	No	LOOP ET	0	5E-4	5E-4
7	No	No	Yes	FLEX-EDG strategy	5.67E-2	2.3E-3	8.7E-6
8	No	No	No	FLEX-ELAP strategy	0.01	1E-2	1.83E-6
Total						1.32E-2	9.4E-4

4 CONCLUSIONS

The numerical values presented in this paper do not represent actual plant data, yet they were selected with reasonable assumptions. For that reason, the final CCDP calculations may not be accurate; however, this case study provides an illustration on how existing safety measures in the plant may be credited to support the objective of a physical protection program. By incorporating an existing infrastructure in the plant towards the PPS' effectiveness, the NPP may have more flexibility in optimizing the PPS infrastructure.

5 REFERENCES

1. Pacific Gas & Electric Company, "PG&E Company 2018 Nuclear Decommissioning Costs Triennial Proceeding Prepared Testimony – Volume 1," https://www.pge.com/pge_global/common/pdfs/safety/how-the-system-works/diablo-canyon-power-plant/diablo-canyon-power-plant/PGE-Nuclear-Decommissioning-Cost-Triennial-20181213-Volume-1.pdf (2018).
2. R. Szilard, P. Sharpe, E. Kee, E. Davis, and E. Grecheck, "Economic and Market Challenges Facing the U.S. Nuclear Commercial Fleet – Cost and Revenue Study," INL/EXT-17-42944, Idaho National Laboratory (2017).
3. U. S. Nuclear Regulatory Commission, "§ 73.55 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 (2021).
4. "AVERT Physical Security," https://aressecuritycorp.com/avert (2020).
5. R. Christian, S. R. Prescott, V. Yadav, S. W. St Germain, and J. Weathersby, "Methodology and Application of Physical Security Effectiveness Based on Dynamic Force-on-Force Modeling," INL/EXT-20-59891, Idaho National Laboratory (2020).