Risk-informed Physical Security Assessment for Nuclear Power Plants

Vaibhav Yadav, Robby Christian, Steven Prescott, and Shawn St. Germain
Idaho National Laboratory, Idaho Falls, USA
vaibhav.yadav@inl.gov, robby.christian@inl.gov, steven.prescott@inl.gov,
shawn.stgermain@inl.gov.

Abstract: The concept of risk-informed physical security for nuclear power plants (NPPs) has recently been extensively explored across various stakeholders, including the nuclear industry, the Department of Energy, the Nuclear Energy Institute, the Nuclear Regulatory Commission (NRC), and researchers at national laboratories and universities. Risk-informed physical security holds promise for advanced assessment and optimization of NPP physical security postures, leading to safer, more efficient, and more economical plant operations. Recently NRC issued a revision to Regulatory Guide 5.76, transitioning from the prescriptive regulatory requirements for physical security to newer guidance based on a reasonable assurance of protection time. The new NRC guidance paves the way for physical security performance assessments to be tied-in with existing risk-based plant safety approaches and associated metrics (e.g., time to core damage) through timeline. This paper presents a novel computational framework for risk-informed physical security, aimed at performing various types of analyses such as security design optimization, armed-guard reduction, and the crediting of plant mitigating strategies in security postures.

1. INTRODUCTION

Overall operation and maintenance costs to protect nuclear power plants (NPPs) account for approximately 7% of the total cost of power generation, with labor accounting for half of this cost [1][2]. As part of research being conducted at Idaho National Laboratory, interaction with utilities and other stakeholders led to the determination that physical security forces account for nearly 20% of the entire workforce at several NPPs [2]. In other aspects of plant operations, risk-informed methods have been deployed to increase safety and reduce inefficiencies. In the realm of physical security, no standard method exists for conducting a risk-informed assessment of a physical protection system (PPS). Such an assessment would readily allow plants to evaluate physical security postures in light of plant risk surrogates such as core damage. Risk-informed physical security holds promise for advanced assessment and optimization of NPP physical security postures, leading to safer, more efficient, and more economical plant operations.

The approach taken by the Nuclear Regulatory Commission (NRC) and the nuclear industry in regard to maintaining effective plant security includes various security programs, each with its own individual objectives. When combined, these programs provide a holistic approach to maintaining effective plant security. The requirements document 10 CFR 73.55(d)(1) states that "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 in onsite response force personnel across the nuclear industry [3]. A plant's response force will include at least the minimum number of armed responders required by 10 CFR 73, along with security officers tasked with assigned duties, including stationary observation/surveillance posts, foot patrol, roving vehicle patrols, compensatory posts, and other duties, as required [4].

Recently, NRC issued a revision to Regulatory Guide 5.76, transitioning from the prescriptive regulatory requirements for physical security to newer guidance based on a reasonable assurance of

protection time [6]. The new NRC guidance paves the way for physical security performance assessments to be tied-in with existing risk-based approaches to plant safety and associated metrics (e.g., time to core damage). The following are the broad benefits of risk-informed physical security: (1) licensees can better focus on protecting the more risk-significant elements of target sets, (2) licensees can optimize their physical security postures by using risk insights, and (3) the inherent subjectivity of current prescriptive regulatory requirements is addressed by connecting physical security effectiveness with risk surrogates such as core damage. Overall, the concept of risk-informed physical security provides security stakeholders with tools and analytical capabilities for performing qualitative and quantitative assessments of plant security postures.

This paper presents a conceptual framework for risk-informed physical security assessments and their application in assessing and optimizing physical security postures at currently operating NPPs, as well as in designing security postures for future reactor sites. Section 2 presents the theoretical foundation for risk-informed security, and Section 3 presents the dynamic modeling of risk-informed security, along with case studies, followed by a framework for applying risk-informed security to the design of security postures at new reactor sites. Section 4 presents a methodology for developing human-action timeline distributions for physical security modeling. Section 5 summarizes this research and presents future work in this area.

2. RISK-INFORMED PHYSICAL SECURITY

For NPP facilities, adversarial attack pathways can be evaluated by simplifying the facilities via an adversary sequence diagram (ASD) model [7]. Figure 1 illustrates an ASD of a hypothetical facility. The ASD transforms the facility layout into a diagram comprised of different areas, with barrier blocks separating each area. Each block in the diagram is assigned a detection probability (P_D) and traversal time (T). These values are evaluated independently for each area or barrier and are typically conservative. An attack timeline can be created based on the ASD diagram, as illustrated in Figure 2.

Figure 1. Adversary sequence diagram.

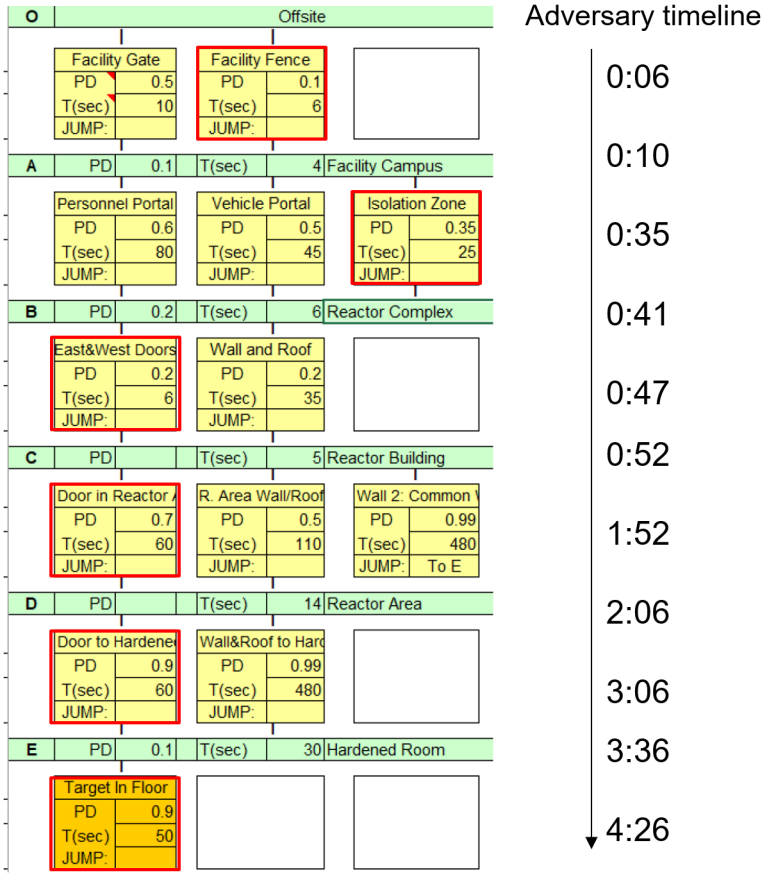
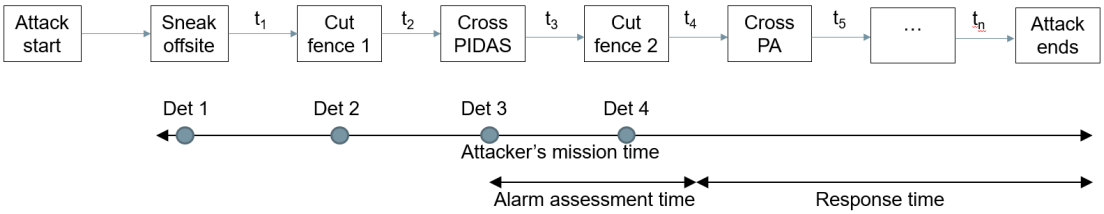


Figure 2. Adversarial attack timeline.



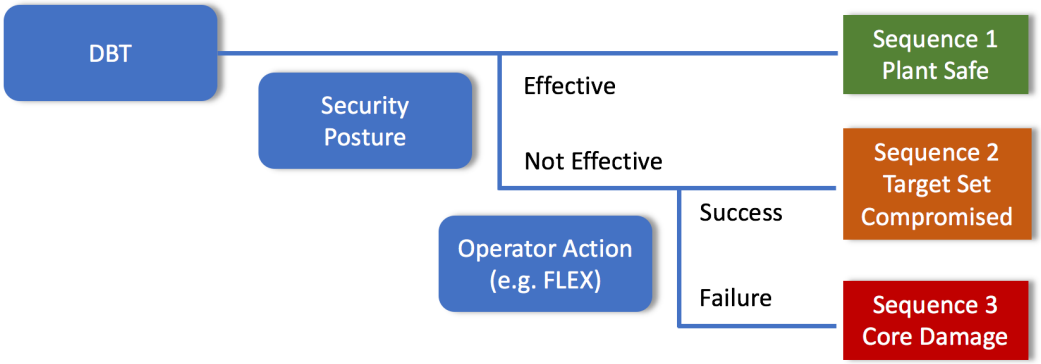
The cumulative probability that the PPS will intercept the adversaries before they complete their attack is given by the probability of interruption: $P_I = 1 - \prod_i (1 - P_D)_i$, where i indicates the ith deterrence. PPS effectiveness is calculated as follows: $P_E = P_I \times P_N$, where P_N is the probability that the response force will neutralize the attackers. The advantages of this methodology stem from its simplicity and ease of use. However, it is a conservative methodology in that it employs simplification of uncertainties, statistical independence, and conservative values for the performance of intrusion detection assessment systems [8]. This conservatism may lead to an overly conservative PPS design. Furthermore, it assumes that the security objective is defeated as soon as the adversaries complete their tasks.

Analogous to the famous risk triplet equation, the risk of an adversarial attack is defined as:

$$Risk = L_A \times [1 - P_E] \times C,$$

where L_A is the likelihood of attack and C is the consequence associated with loss of the targets the PPS is designed to protect. For NPPs, this consequence typically takes the form of core damage or radiological release. The protection measures are considered failed once a target set is successfully sabotaged. Such an approach affords a simplified acceptance criterion for the PPS design objective. However, these criterions are understood to contain a conservative assumption that undermines the period of time that exists between the moment a target set is damaged and when significant core damage or radiological release becomes imminent. Following damage to the target set, operator actions may still prevent core damage or radiological release. Figure 3 illustrates this concept. NPP security programs are designed to protect against design basis threats (DBTs). When a DBT attack occurs, there is a chance that the security system will prove ineffective at preventing the adversary from sabotaging the target set. In such situations, once the threat is removed, operator actions may still prevent core damage, i.e., preventing Sequence 2 from segueing into Sequence 3, per Figure 3.

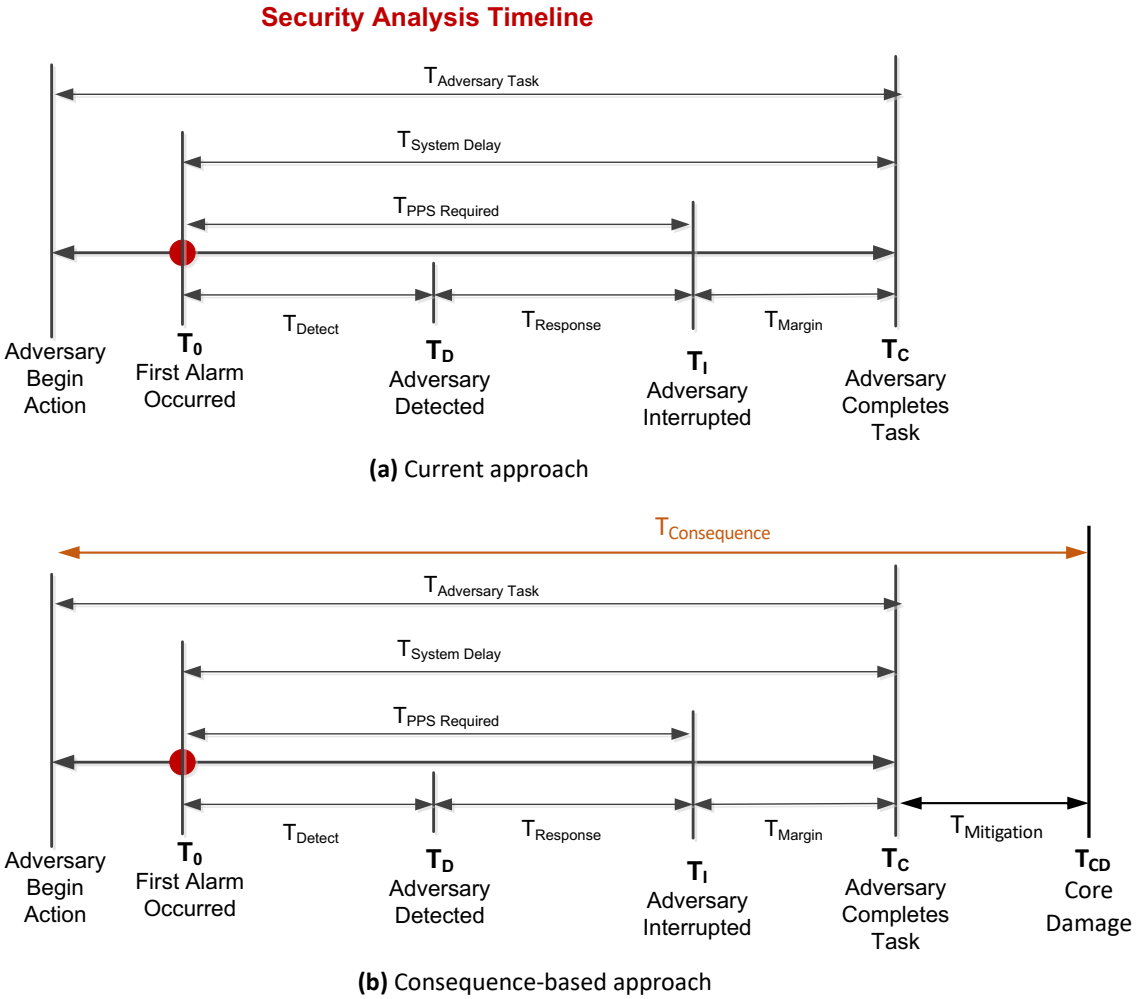
Figure 3. Concept of integrating safety and security programs for risk assessment of security events.



A consequence-based approach to physical security can be implemented to incorporate the aforementioned time margin in which mitigation actions can be performed to prevent plant damage. Figure 4 compares the timeline analysis of the current approach with that of a consequence-based

approach. Under the current approach, the PPS is considered failed if the adversaries successfully complete their task. In the consequence-based approach, the plant can take credit of operator actions to prevent significant core damage even after the target set is compromised. Operator event-mitigation actions can be performed *after* the "Adversary Completes Task" event in Figure 4(a). $T_{Mitigation}$, as shown in Figure 4(b), is the point at which core damage becomes imminent. The plant operator must complete the mitigation actions within $T_{Mitigation}$ to prevent core damage. Such an approach directly connects target element sabotage with consequences such as core damage, enhancing the realism of physical security assessments. The following section presents case studies involving the use of risk-informed physical security based on dynamic modeling and simulation (M&S) of NPP physical security postures.

Figure 4. Comparison between the current and consequence-based approaches to security timeline analysis.



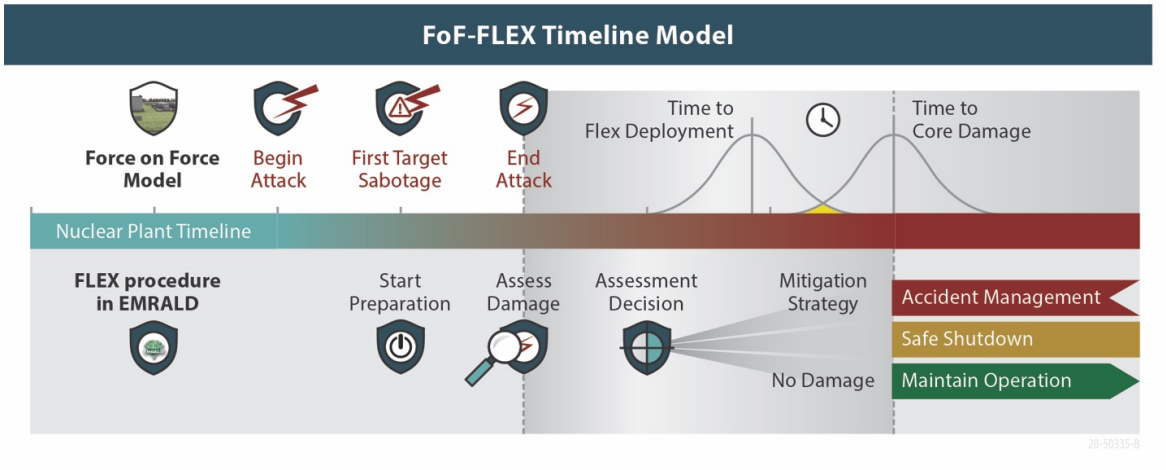
3. DYNAMIC MODELING OF PHYSICAL SECURITY

Risk-informed physical security assessments have been implemented for several applications, including increasing the efficiencies of current security postures, optimizing existing plant security postures, addressing subjectivity in security regulations, and crediting operator actions during security events. This section presents one such application in detail.

The M&S framework for integrating Diverse and Flexible Mitigation Capability Strategies (FLEX) equipment with force-on-force (FOF) models enables NPPs to credit FLEX portable equipment as part of their security postures, resulting in efficient, optimized physical security postures [9]. Figure 5 gives an overview of the dynamic framework for FOF and FLEX model integration, which begins with the

FOF simulation being conducted using a commercial FOF software (see the top half of Figure 5). A typical FOF simulation provides the attack timeline data, as well as the targets' status at the end of the attack. The "End Attack" point in Figure 5 leads to one of two outcomes: target safe or target sabotaged, and the associated time. This outcome is read by Event Modeling Risk Assessment using Linked Diagrams (EMRALD), a dynamic simulation tool, to determine the appropriate timing for beginning preparation of the FLEX portable equipment (see the bottom half of Figure 5). If the attack is unsuccessful, the plant may continue normal operations. If the target is sabotaged, FLEX preparation is initiated, potentially including communication/coordination with field personnel as well as equipment mobilization, staging, and connection. The mobilization and staging phase may be skipped if the FLEX equipment is pre-staged. The required FLEX equipment and associated FLEX procedures are determined during the "Assess Damage" step in Figure 5.

Figure 5. FOF-FLEX integration framework.



Dynamic uncertainties in FLEX preparation, as modeled in EMRALD, create a statistical distribution of the timeline of FLEX equipment being made 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 these data to determine an applicable mitigation strategy, as needed. Meanwhile, if several components or pieces of equipment are sabotaged but the plant still retains its design basis safety functions thanks to intact redundant or standby components, mitigation is carried out by 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. Execution of this FLEX strategy depends on which safety functions are lost following the attack.

This section describes a case study that demonstrates the applicability of the FOF-FLEX integration model. This case study involves a hypothetical attack scenario at a hypothetical pressurized-water reactor plant, and does not utilize any plant proprietary data or information. In the attack scenario, a group of adversaries attempts to cause radiological release by sabotaging the plant's power supply and its ultimate heat sink capabilities. Figure 6 shows the targets and the attack path for inflicting the aforementioned core damage progression.

The attack scenario begins with the adversaries setting explosives at an unmonitored grid tower outside the NPP complex in order to cause loss of offsite power. Concurrently, a group of armed adversaries enters the complex with the intent to sabotage the emergency diesel generators (DGs) in order to cause a station blackout (SBO) event and damage the turbine-driven pumps (TDPs), thus disabling the plant's passive heat removal capability. The plant has a PPS program in place, consisting of an intrusion detection system, delay barriers, and both a stationary and mobile response force. For purposes of visual clarity regarding the attack path and target locations, these protection elements are not shown in Figure 6.

Figure 6. Attack targets and path in the force-on-force model.

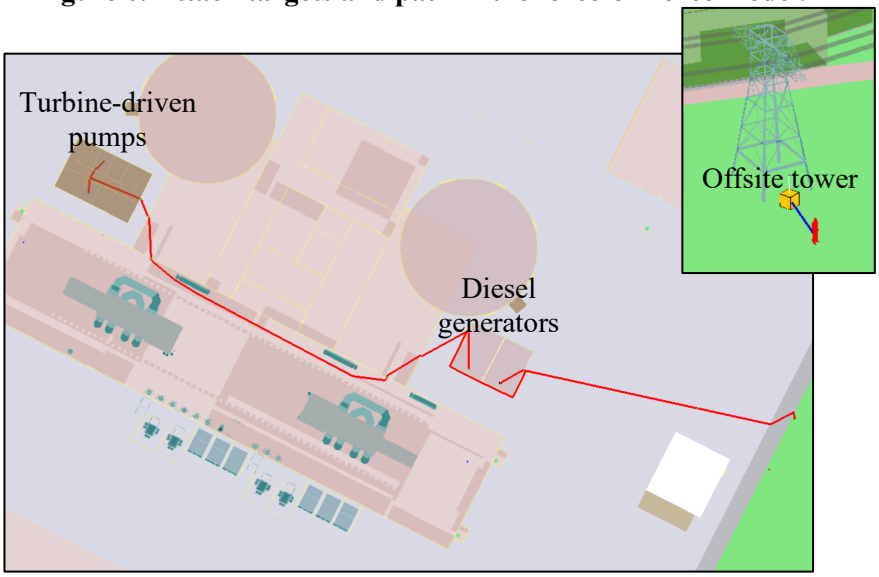
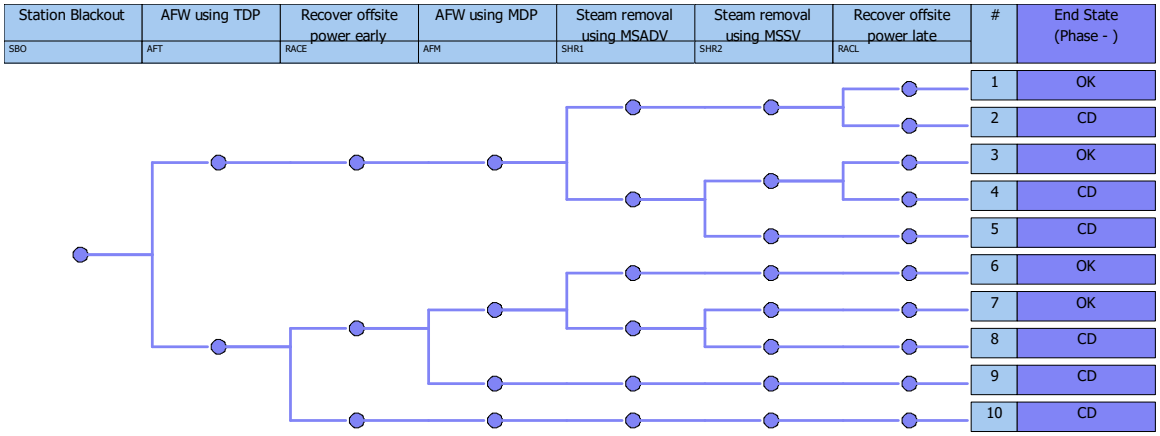


Figure 7. Event tree for an SBO event.



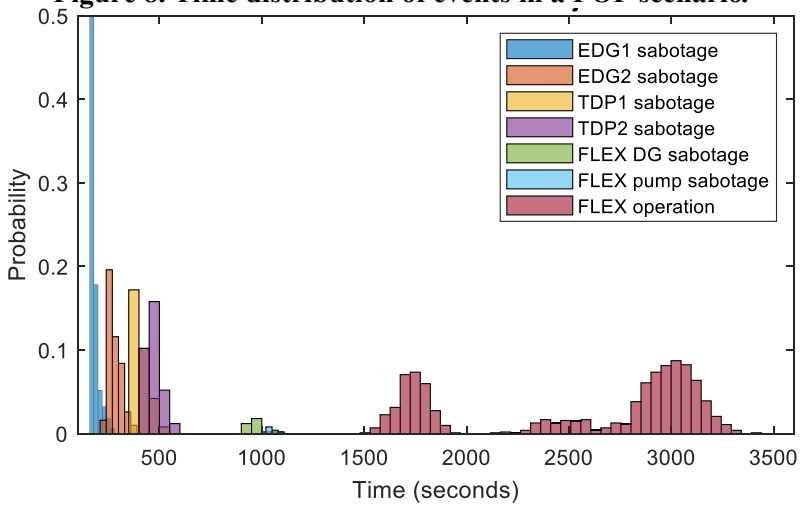
If the plant security posture successfully neutralizes the attack, the plant may continue normal operations, as illustrated by Sequence 1 in Figure 3. However, if a target element is sabotaged and results in a SBO event, plant SOB-event mitigation actions are initiated, as illustrated in Figure 7. If the plant loses one or more safety functions when no safety-related event has been initiated, the plant simply ceases operation in order to repair the damaged safety systems. In light of an initiating safety event, such issues are mitigated by the design basis safety systems, if available. Otherwise, FLEX equipment will substitute for the safety functions of the damaged design basis systems. The FLEX strategy entails utilizing the FLEX DG to provide power, while FLEX pumps supply feedwater to the plant's secondary side. The time durations associated with performing FLEX strategies can be obtained from plant-specific procedures or from a reference study [10].

Table 1 shows the typical procedure for implementing a FLEX strategy. The FLEX equipment is assumed to be pre-staged and not stored in a storage building; thus, it does not need to be moved. The steps in this procedure are categorized as pertaining to either the preparation or execution stage of the FLEX strategy. After the FOF simulation is complete, an assessment is conducted to determine the plant status. Based on this assessment, the appropriate FLEX strategy is performed, following the execution actions listed in Table 1. Based on the plant-specific FLEX procedure, each step in Table 1 will correspond to a statistical distribution of time associated with carrying it out.

Table 1. Typical procedure for implementing a FLEX strategy.

	Steps	Notes
1	Get keys and open doors	Preparation
2	Assess condition of plant system & equipment	Execution
3	Connect FLEX pump to inject coolant to steam generators	Preparation
4	Establish configuration to support FLEX 480-V AC installation	Execution
5	Connect FLEX cables to 480-V Motor Control Center (MCCs)	Preparation
6	Open all breakers on MCCs	Execution
7	Connect FLEX RCS Makeup pump hoses	Preparation
8	Inform Security of security area access breaches	Execution
9	Put a FLEX DG in service	Preparation
10	Restore partial lighting and receptacle power	Execution
11	Turn on the supply breaker in the FLEX DG enclosure	Preparation
12	Evaluate potential uses of the portable equipment being delivered from RRC	Execution
13	Ensure that the support equipment is staged	Preparation
14	Establish communication	Execution

Figure 8. Time distribution of events in a FOF scenario.



A computational simulation that sampled across the distribution of operator actions and integrated with the FOF model simulation was performed using EMRALD. The simulation produced a time distribution for different FOF outcomes, as shown in Figure 8. Operators began initiating the FLEX procedure as soon as the respective safety function from the design basis equipment was lost. Because the adversaries sabotaged TDP pumps after the DGs, the histogram of FLEX operation has two distinct peaks corresponding to the timing when safety functions of the DGs and TDP pumps were lost.

Thermal-hydraulic analysis of FLEX systems can realistically estimate the time to core damage by taking into account the uncertainties in safety system actuation and operator performance. These uncertainties are incorporated into the thermal-hydraulic analysis to simulate the plant response when adversaries successfully sabotage all the equipment in the target set. In this case study, a typical 1000-MW NPP model was simulated in RELAP5 [7], and the details are available in [8]. Besides the uncertainties in human operator actions, random failures (e.g., failure to start and failure to run continuously) create additional uncertainties in terms of safety system/component performance. These uncertainties are statically modeled in the plant's probabilistic risk assessment model, but are incorporated dynamically in the thermohydraulic model to estimate the core damage timing [8].

Thermohydraulic analysis in RELAP5 is performed by applying the grid-sampling method to the operator-action timeline and uncertainty sources listed in Table 2. A safety limit for the peak cladding temperature, as computed by RELAP5, is selected to determine whether the reactor core has been damaged. For each core-damage outcome, the thermohydraulic simulation in RELAP5 estimates the time to core damage, which can be used to obtain the distribution of time to core damage.

4. RISK-INFORMED RESULTS AND INSIGHTS

Traditional security assessments using FOF analysis generate results in the form of binary outcomes (e.g., the security posture was successful or unsuccessful at preventing sabotage). Insights derived from such analyses are limited and not related to plant risk. Via the risk-informed security approach, plants can produce security outcomes that are no longer binary but instead take the form of probabilities or timelines (Figure 8), as well as connect security outcomes to risk surrogates such as core-damage frequency. This section presents a snapshot of the results and insights obtained from risk-informed security M&S, which can aid plants in optimizing their security postures without compromising plant safety.

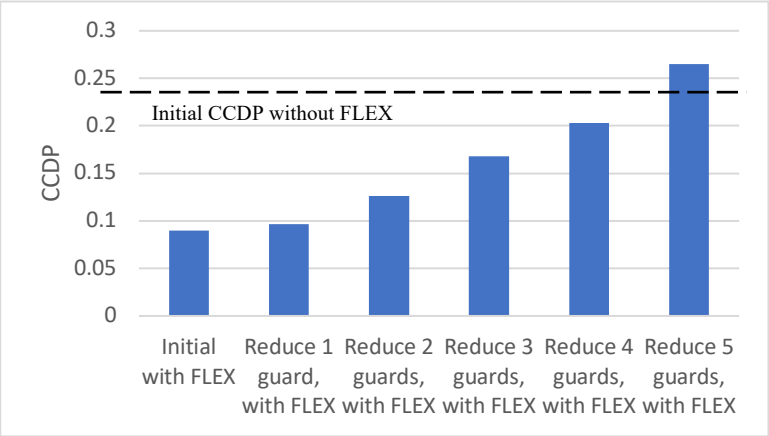
The methodology shown in Section 3 is applied to several different types of attack scenarios, and the results can be compared to assess security effectiveness and plant safety across those scenarios. Table 2 gives an example of outcomes obtained by running four scenarios: A–D. The table compares importance measures of each scenario, potentially aiding plant security by identifying the most significant scenario on which to focus, along with the cumulative core damage probability (CCDP) for each scenario. As expected, the CCDP is significantly reduced by integrating FLEX strategies with plant security postures, thus providing plants with quantitative insights into the gained safety margin.

Table 2. Overall adversary success probability in beyond-DBT attack scenarios.

Scenarios	Importance Measure		CCDP	
	Without FLEX Strategy	With FLEX Strategy	Without FLEX Strategy	With FLEX Strategy
Scenario A	38.48%	14.25%	3.29E−01	4.00E−02
Scenario B	28.60%	11.61%	2.45E−01	3.26E−02
Scenario C	11.46%	27.08%	9.80E−02	7.60E−02
Scenario D	21.46%	47.06%	1.84E−01	1.32E−01
Total	100.00%	100.00%	6.27E−01	2.55E−01

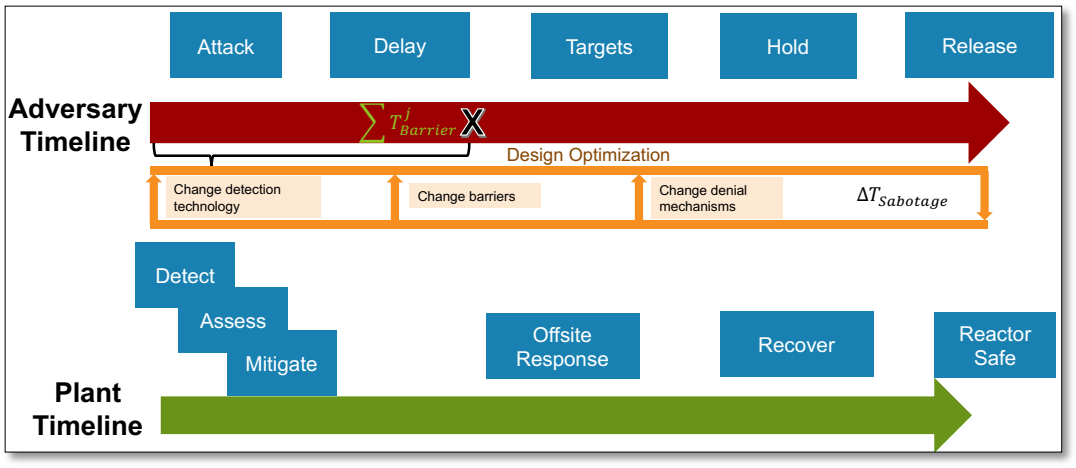
The CCDP values for security scenarios can be further utilized to optimize plant security postures. Figure 9 illustrates an iterative process for determining the least effective posts, revealing that four posts can be excluded from the response force while still maintaining the adversary success probability below the initial adversary success probability. When five posts are removed, the adversary success probability exceeds the initial adversary success probability; thus, that configuration can be seen as the stopping point in the iterative optimization process.

Figure 9. Adversary success probability and margin.



The concept of an iterative process of security posture optimization is currently being employed for optimizing the design of security postures for advanced reactor sites. Ongoing research efforts at INL are being conducted to develop a computational framework for risk-informed security that integrates security timeline estimations with plant security design elements' effectiveness, as well as that of the security posture as a whole. Figure 10 shows an approach that hinges on modeling the intersection of two distinct timelines (i.e., the Adversary Timeline and the Plant Timeline) during an attack scenario. The Adversary Timeline follows the adversaries and models the timings of adversarial actions, e.g., initiation of attack, adversary delay at each barrier, time it takes for an adversary to reach a target, time to engage an adversary, ending in the unlikely outcome of time to release. The Plant Timeline model incorporates when plant capabilities are initiated, such as time to detection and assessment of attack, time to initiate mitigation action, time for offsite responders to arrive, and time for plant to recover. The intersection of the two timelines can be utilized to define the effectiveness of a security posture. The sensitivities of each security element to the posture's overall effectiveness can be then used to optimize the security elements. This is a work in progress, and more insights will be available at a future time.

Figure 10. Illustration of security posture design optimization based on security timeline estimation.



4. CONCLUSION

This paper presented a conceptual and applied framework for risk-informed assessments of NPP physical security postures. A case study on integrating physical security FOF models with plant FLEX equipment demonstrated that, even in the extreme case of a successful adversarial attack, deployment of FLEX equipment entails a significantly high likelihood of preventing radiological release. The M&S framework for integrating FLEX equipment with FOF models enables NPPs to credit FLEX portable

equipment in their security postures, resulting in efficient and optimized physical security. The following are the broad benefits of risk-informed physical security: (1) licensees can better focus on protecting the more risk-significant elements of target sets, (2) licensees can optimize their physical security postures by using risk insights, and (3) the inherent subjectivity of current prescriptive regulatory requirements is addressed by connecting physical security effectiveness with risk surrogates such as core damage. Overall, the concept of risk-informed physical security provides security stakeholders with tools and analytical capabilities for performing qualitative and quantitative assessments of plant security postures.

Ongoing and future efforts in this area include (1) implementing this framework in the physical security posture and FLEX equipment of a specific plant, (2) modeling the FLEX equipment and enclosure as a target set in the physical security posture, (3) integrating human reliability analysis into the dynamic model, and (4) optimizing security posture designs at future reactor sites.

Acknowledgements

This research was supported through the U.S. Department of Energy's Light Water Reactor Sustainability program.

References

[1] Pacific Gas and Electric Company. *"PG&E Company 2018 Nuclear Decommissioning Costs Triennial Proceeding Prepared Testimony – Volume 1,"* 18-12 (U 39 E), PG&E Company, (2018).

[2] R. Christian, S. R. Prescott, V. Yadav, S. W. St Germain, C. P. Chwasz. *"Integration of Physical Security Simulation Software Applications in a Dynamic Risk Framework,"* INL/EXT-21-64333, Idaho National Laboratory, (2021).

[3] U.S. Nuclear Regulatory Commission. *"Emergency Preparedness in Response to Terrorism,"* About Emergency Preparedness, (2020). https://www.nrc.gov/about-nrc/emerg-preparedness/about-emerg-preparedness/response-terrorism.html#one.

[4] U.S. Nuclear Regulatory Commission. *"PART 73—Physical Protection of Plants and Materials,"* Regulations, (2021). https://www.nrc.gov/reading-rm/doc-collections/cfr/part073.

[5] U.S. Nuclear Regulatory Commission. *"Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage,"* Regulations, (2021). https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0055.html.

[6] U.S. Nuclear Regulatory Commission. *"Physical Protection Programs at Nuclear Power Reactors,"* 85 FR 76625, U.S. Nuclear Regulatory Commission, (2020).

[7] Y. A. Setiawan. *"Adversary Path Analysis of a Physical Protection System Design Using a Stochastic Approach,"* MS Thesis, Texas A&M University, (2018).

[8] R. Christian, S. R. Prescott, V. Yadav, S. W. St Germain, J. Weathersby. *"Methodology and Application of Physical Security Effectiveness Based on Dynamic Force-on-Force Modeling,"* INL/EXT-20-59891, Idaho National Laboratory, (2020).

[9] Nuclear Energy Institute. *"Diverse and Flexible Coping Strategies (FLEX) Implementation Guide,"* NEI 12-06, Nuclear Energy Institute, (2015).

[10] D. Kang and S. Chang. *"The safety assessment of OPR-1000 nuclear power plant for station blackout accident applying the combined deterministic and probabilistic procedure,"* Nuclear Engineering and Design, volume 275, pp. 142–153, (2014).