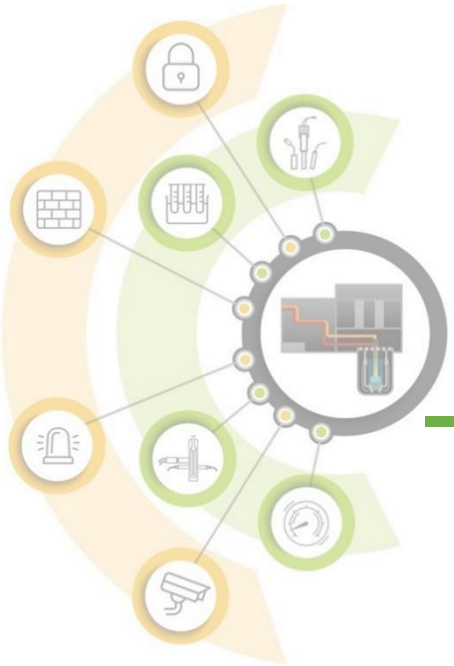


Physical Security Timeline Analysis in Support of Advanced Reactor Demonstration and Deployment

Prepared for
U.S. Department of Energy

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

Idaho National Laboratory

February 2023
INL/RPT-23-71219

INL/RPT-23-71219
Revision 0

Physical Security Timeline Analysis in Support of Advanced Reactor Demonstration and Deployment

Robby Christian
Steven R. Prescott
Vaibhav Yadav
Shawn W. St Germain
Christopher P. Chwasz

February 2023

Prepared for the
U.S. Department of Energy

ABSTRACT

This report presents the regulatory requirements and directions on the physical security of advanced nuclear reactors in the United States. Presently, a rule is being proposed that allows for a performance-based analysis of physical security posture. In determining the physical security requirements for an advanced reactor, new tools may be desired to conduct a performance-based analysis. These tools should incorporate dynamic analysis methods to provide as much realism as possible. In comparison, the security requirements for existing light-water reactors are much more prescriptive, and the analysis conducted to establish the required physical security strategies are more easily performed with static analysis. To achieve the cost goals that advanced reactors require for adoption, the nuclear security force required should not be excessive. Dynamic physical security analysis methods and tools have been developed by the U.S. Department of Energy's Light Water Reactor Sustainability program. This report details how the dynamic risk analysis tools developed in this program using the dynamic risk modeling tool, Event Modeling Risk Assessment using Linked Diagrams (EMRALD), may be adapted for use in analyzing the physical security designs for advanced reactors accounting for variable performance-based requirements. This report provides an example analysis of a **hypothetical sodium-cooled fast reactor using publicly available information and generic assumptions** to demonstrate the methods and potential presentation and analysis of the results. **No actual plant information is used in this example analysis**. Future work in this area will create additional models that can be adapted for any advanced reactor concept and use various security features to create a physical security system that provides adequate protection from radiological theft and sabotage.

Page intentionally left blank

CONTENTS

FIGURES

TABLES

Page intentionally left blank

ACRONYMS

BRE	Bullet Resistant Enclosures
CDP	Critical Detection Point
CFR	Code of Federal Regulations
DOE	Department of Energy
DPRA	Dynamic Probabilistic Risk Assessment
EASI	Estimate of Adversary Sequence Interruption
ESFR	Example Sodium Fast Reactor
EMRALD	Event Modeling Risk Assessment using Linked Diagrams
FLEX	Diverse and flexible coping strategies
FOF	Force-On-Force
GUI	Graphical User Interface
INL	Idaho National Laboratory
LWR	Light Water Reactor
LWRS	Light Water Reactor Sustainability
MASS-DEF	Modeling and Analysis for Safety Security using Dynamic EMRALD Framework
NEI	Nuclear Energy Institute
NEIMA	Nuclear Energy Innovation and Modernization Act
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
PE	Probability of Effectiveness
PI	Probability of Interruption
PIDAS	Perimeter Intrusion Detection and Assessment System
PPS	Physical Protection System
PRA	Probabilistic Risk Assessment
SAPHIRE	Systems Analysis Programs for Hands-On Integrated Reliability Evaluations
SECY	Commission papers
SCS	Shutdown Cooling System
SFR	Sodium-cooled Fast Reactor
TRU	Transuranic

Page intentionally left blank

PHYSICAL SECURITY TIMELINE ANALYSIS IN SUPPORT OF ADVANCED REACTOR DEMONSTRATION AND DEPLOYMENT

1. INTRODUCTION

1.1 Regulatory Background

The U.S. Nuclear Regulatory Commission (NRC) has been on the path to implement performance-based regulation of commercial nuclear reactors for the last three decades. The increased safety of advanced reactors and advances in modeling has precipitated a mandate in the Nuclear Energy Innovation and Modernization Act (NEIMA) for the NRC to initiate fully performance-based licensing methodologies. The Department of Energy (DOE) and industry's cost-shared Technology Inclusive Content of Application Project uses the Licensing Modernization Project's frequency- and consequence-based event and structures, systems, and components categorization outlined in Nuclear Energy Institute (NEI) 18-04, Rev. 1 to provide a framework for the performance-based licensing of commercial nuclear power plants (NPPs) [1]. The NRC has endorsed this methodology for Part 50 [2] and 52 [3] commercial nuclear power reactor licenses in Regulatory Guide 1.233 [4]. The NRC staff has also initiated 10 CFR Part 53 to establish a fully performance-based licensing framework [5].

The U.S. nuclear industry also expressed interest in the use of performance-based regulation for the physical security of commercial nuclear reactors, as described in the 2018 NEI white paper, *Proposed Physical Security Requirements for Advanced Reactor Technologies* [6]. Currently, the fleet of large light-water reactors (LWRs) has numerous prescriptive requirements to ensure the secure operation of commercial nuclear reactors against the design basis threat of radiological sabotage. Included within the requirements are performance criteria to prevent core damage and spent fuel sabotage. Licensees design their physical protection systems (PPSs) to meet these performance criteria, fulfill the prescriptive requirements found in 10 CFR Part 73.55 [7], and pass NRC inspections and exercises. The NRC staff reviewed the whitepaper and provided options to the commission in SECY 18-076 [8]. As a result, the NRC initiated a limited-scope rulemaking to establish alternatives for the physical protection of commercial NPPs.

The limited-scope physical security rulemaking (NRC-2017-0227) was initiated to provide a performance-based alternative for advanced reactors that can demonstrate higher safety performance to meet physical security requirements [9]. The proposed rule is currently before the commission for approval, per SECY-22-0072 [10]. The current language in the proposed rule requires that:

> The applicant or licensee must demonstrate that the consequences of a postulated radiological release that results from a postulated security-initiated event do not exceed the offsite dose reference values defined in §§ 50.34 and 52.79 of this chapter.

1.2 Stakeholder Workshop

Idaho National Laboratory (INL) staff attended the Advanced Reactor Safeguards stakeholder workshop hosted at Sandia National Laboratory in October 2022. INL discussed this work with physical security modeling firms, national laboratory staff, and advanced reactor physical security designers and managers. The intention of security-by-design was discussed extensively, as well as the dearth of methodologies and guidance to credit the plant security-by-design aspects in a protective strategy.

1.3 Research Objective

With the recent research focused at supporting the development, demonstration, and deployment of advanced nuclear reactors, it is necessary to research the security aspect of advanced reactors. The goal of

security analysis at the beginning stages of the advanced reactor life cycle is to prevent expensive retrofits in the latter stages and demonstrate compliance with the regulations. This study aims to provide a physical security analysis methodology of a generic sodium-cooled fast reactor (SFR) design by leveraging previous security analysis experience for LWRs [11][12]. The proposed physical security analysis methodology should demonstrate how an alternative physical security protective strategy to that listed in 10 CFR 73.55 can be shown to comply with the dose reference values in 10 CFR 50.34 [13] and 52.79 [14] during and after a design basis attack of radiological sabotage, consistent with the requirements of the proposed limited-scope physical security rulemaking. The implementation of the methodology for a generic SFR is the subject of future work.

2. DYNAMIC ANALYSIS IN PHYSICAL SECURITY

Current risk assessments for nuclear application are limited since they do not properly consider changes in risk scenarios over time. Any system reliability that depends heavily on the timing of component failures, orders of failures, or operator actions could greatly benefit from dynamic risk analysis. Examples include dam failure and consequence analysis, power grid reliability, supply chain analysis, etc. Event Modeling Risk Assessment using Linked Diagrams (EMRALD) is a dynamic risk analysis tool developed at INL and has been successfully implemented for use cases such as seismic analysis, pipe rupture, flooding, and force-on-force (FOF) analysis of current plant security posture [11] [12] [15].

Extending these risk analysis methods into the creation of dynamic security scenarios to represent the advanced reactor physics provides scenario-based analyses that include the treatment of associated uncertainties. Uncertainties found in scenarios are captured by automating the state space (i.e., various potential plant conditions) meaning that computational approaches can represent a vast array of different boundary and operational conditions. In dynamic analysis of security scenarios at currently operating NPPs, EMRALD has been applied to manage the different FOF simulation tools and supplement the simulation capabilities with dynamic uncertainties, as shown in Figure 1.

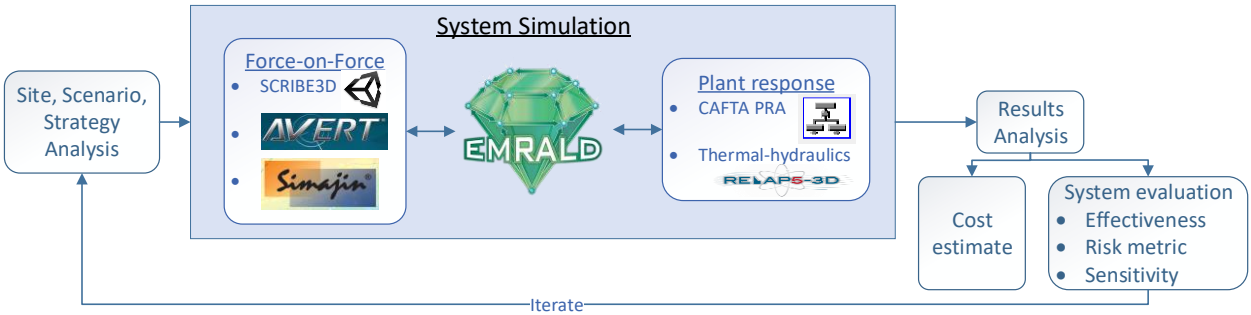


Figure 1. Outline of the dynamic framework.

This framework allows a security analyst to identify the excess conservatism in their security posture and gain further insight on optimizing the posture for protection effectiveness and associated costs. The following are examples of analyses that may be performed using this framework:

1. Demonstrating minimal impact to security effectiveness using randomized shift breaks
2. Evaluating the potential cost savings or performance improvements for implementing new physical security features such as bullet resistant enclosures (BREs)
3. Optimizing the placement of BREs on a site
4. Analyzing operator actions to mitigate sabotage attacks, such as:

a. The likelihood and possible pathway for control room operators to evacuate to a backup control room under certain circumstances

5. Crediting diverse and flexible coping (FLEX) mitigation strategies
6. Evaluating the effectiveness of potential new security technologies such as advanced non-lethal delay devices or remote-operated weapons systems.

The dynamic methodology used to analyze the physical security of LWRs is named Modeling and Analysis for Safety Security using Dynamic EMRALD Framework (MASS-DEF). The following subsection introduces the EMRALD tool used in this methodology.

2.1 EMRALD

To accurately assess attack scenarios and reactor consequences, time dependent dynamic modeling is needed. The modeling tool chosen for this work is EMRALD which is a tool designed to enable the modeling of complex time dependent interactions between system and/or human actions, using a drag-and-drop node-based graphical user interface (GUI). EMRALD consists of two main pieces, the web-based model builder GUI and the simulation solver. Results show how events over time lead to critical outcomes along with the probabilities.

2.1.1 EMRALD Modeling

The model building interface was designed to help visualize dynamic probabilistic risk assessment (DPRA) flow and make the process as similar to traditional probabilistic risk assessment (PRA) as possible [15]. There are many pieces that make up an EMRALD model.

2.1.1.1 Diagrams

An EMRALD model consists of multiple diagrams. Each diagram represents a particular piece of the model and various conditions or states that this piece of the model can be in. These pieces correlate to aspects of traditional PRA modeling and range from small-scale components to a large scope of plant response and design as shown in Figure 2. A diagram contains multiple states with events that can occur and actions that may be executed. These all define how the current states of the simulation may shift over time. The different diagrams can affect each other by changing variable values or through different types of events. For example, an event can evaluate if a pump is in an active or failed state.

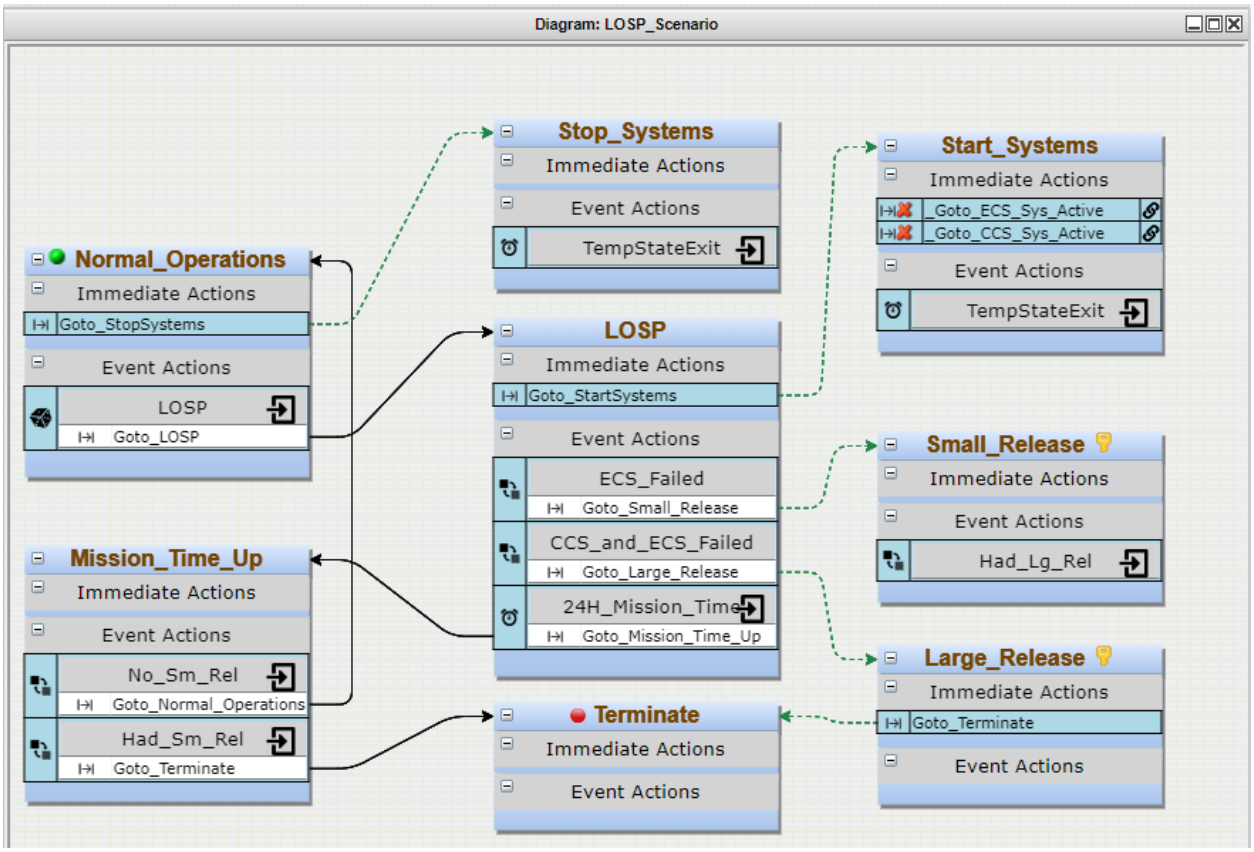


Figure 2. An EMRALD plant diagram showing a loss of offsite power scenario.

Additionally, some diagrams (component and state diagrams) can also be evaluated for a Boolean result depending on which state they are currently in, as shown in Figure 3. This is a critical feature that, when combined with a component logic event, can greatly simplify a model and prevent exponential size growth that happens with typical Markov models.

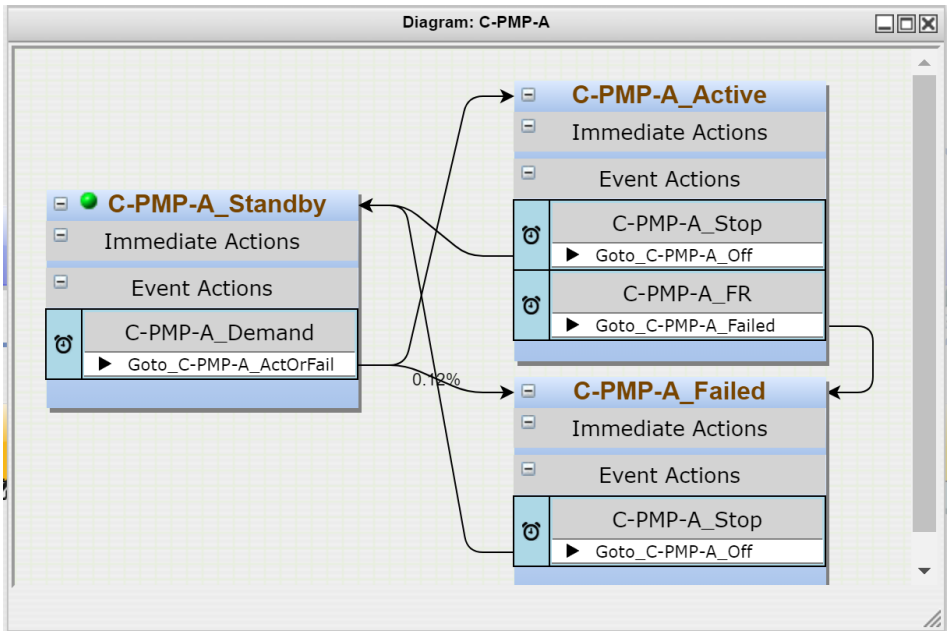


Figure 3. Example of a component diagram and the different states it can be in.

2.1.1.2 State Events and Actions

States are a logical representation for a current condition in a diagram. Each state has or can have the following attributes:

- Type – start, standard, key state, or terminal, which establishes simulation behavior when setting up, running, or post-processing a simulation run
- Immediate Actions – actions that are executed when entering the state
- Event Actions – items to monitor when in this state which can then trigger one or more actions.

Events are what a state is looking for to trigger something. There are two categories of events: time based and condition based. Time-based events sample the next time to failure, such as a probability distribution. Condition events are evaluated every time something that could impact the event changes, such as evaluating if a variable is below a specified value. If a state is marked as a key state, then this state is tracked for results.

Actions are things that can be done in the simulation space, such as changing a variable value, transitioning to a different state, or running a thermal hydraulics code. Actions are taken when entering a state or are linked to an event and are executed after that event occurs.

Whenever EMRALD enters a new state during a simulation, the immediate actions are executed, and the events are either sampled and put in the time queue or added to an evaluation list to see if they are triggered. When exiting a state, all its events are no longer valid and are removed. Additional events or actions could be added to EMRALD to handle coupling with Systems Analysis Programs for Hands-On Integrated Reliability Evaluations (SAPHIRE) and process results.

2.1.2 EMRALD Simulation Process

EMRALD is a discrete event method, where the simulation jumps to the next event in time, which is ideal for simulations that can have varying time intervals in their simulation space. Specifically, it uses a three-phase discrete event simulation [16] with the evaluation steps shown in Figure 4. Statistical results are determined by compiling the outcome of many Monte-Carlo simulation runs.

Upon loading, initial start states are added to the “Current” and “New States” list.

1. While there are states in the “New States” list, For each state:
   - Add the events to the “Time Events Queue” or “Conditional Events” list.
   - Execute any Immediate Actions

2. If any “Conditional Events” criteria is met.
   - Execute that events action/s.
   - Go to Step 1.

3. Jump to the next chronological event.
   - Process that event’s actions.
   - Go to Step 1.

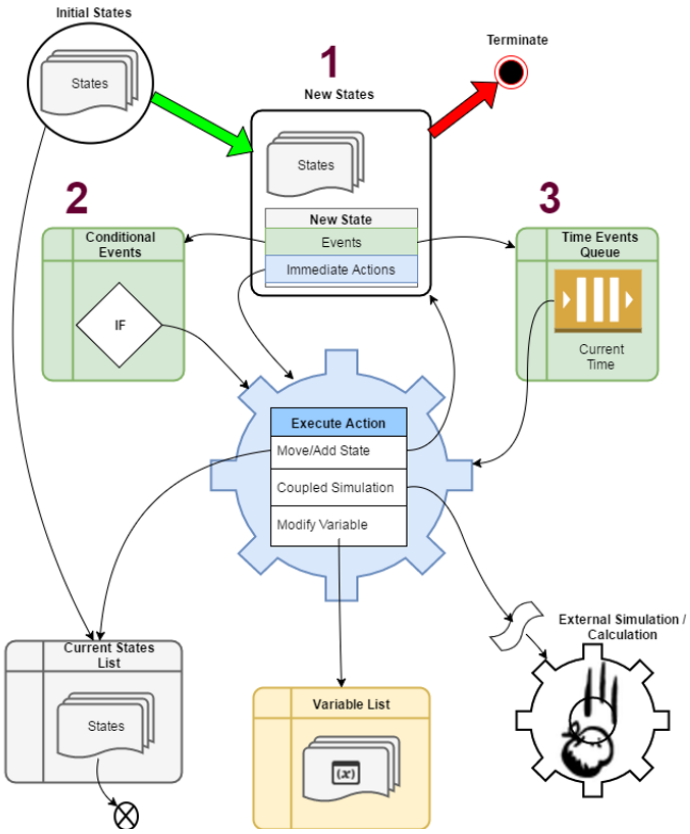
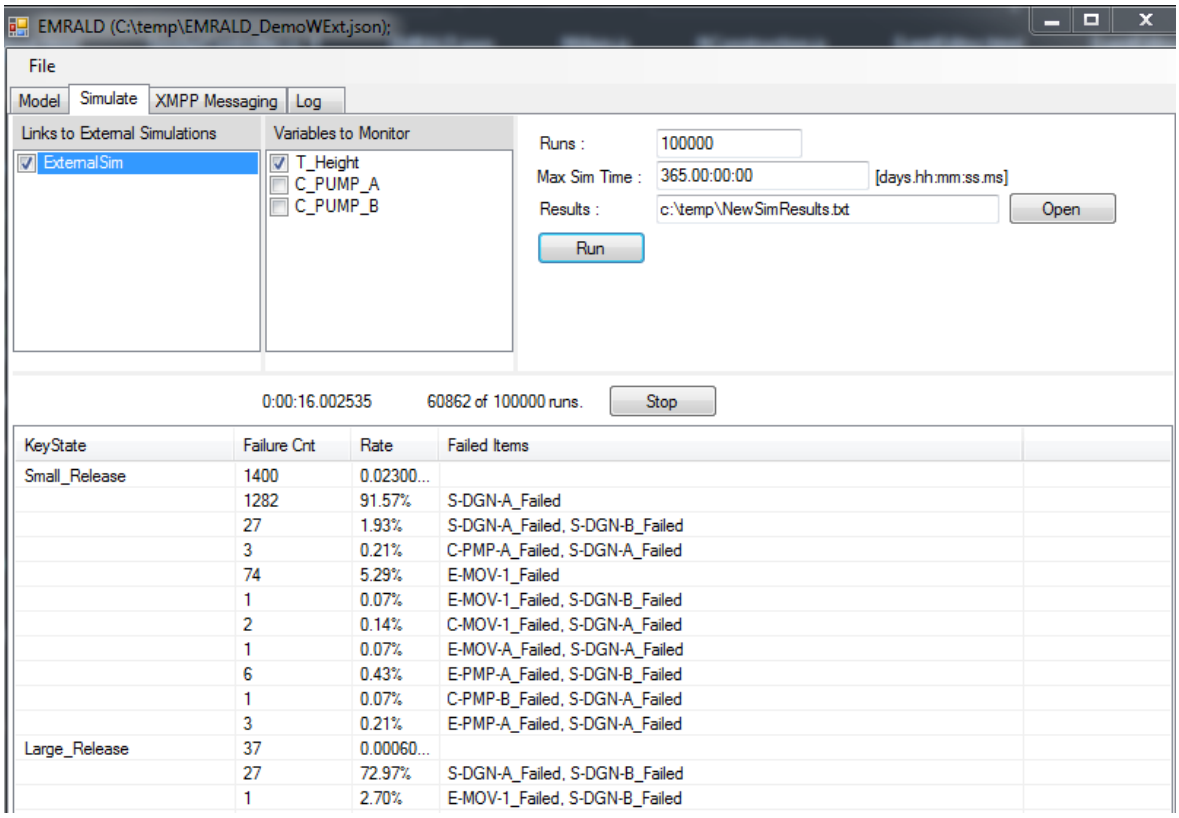


Figure 4. EMRALD simulation process based on three-phase discrete event simulation.

Each simulation loads the model and processes through the steps until a terminal state or the max simulation time is reached. When a simulation ends, any states that the simulation is currently in are saved for the results. The path and timing for how that state entered are saved. With multiple simulation runs, statistical data can determine the probability of ending in a key state vs. how many simulation runs were executed.

The solve engine, shown in Figure 5, is used to run the model. The user specifies the max simulation time and any variables they want to monitor. A compiling of the simulation runs into overall results shows all the paths and timings that caused the model to end in one of the key states. Results can also show the different combinations of component states that were encountered for the key states, as shown in the bottom section of Figure 5.



KeyState	Failure Cnt	Rate	Failed Items
Small_Release	1400	0.02300...	
	1282	91.57%	S-DGN-A_Failed
	27	1.93%	S-DGN-A_Failed, S-DGN-B_Failed
	3	0.21%	C-PMP-A_Failed, S-DGN-A_Failed
	74	5.29%	E-MOV-1_Failed
	1	0.07%	E-MOV-1_Failed, S-DGN-B_Failed
	2	0.14%	C-MOV-1_Failed, S-DGN-A_Failed
	1	0.07%	E-MOV-A_Failed, S-DGN-A_Failed
	6	0.43%	E-PMP-A_Failed, S-DGN-B_Failed
	1	0.07%	C-PMP-B_Failed, S-DGN-A_Failed
	3	0.21%	E-PMP-A_Failed, S-DGN-A_Failed
Large_Release	37	0.00060...	
	27	72.97%	S-DGN-A_Failed, S-DGN-B_Failed
	1	2.70%	E-MOV-1_Failed, S-DGN-B_Failed

Figure 5. EMRALD solve engine interface and summary results.

2.2 LWRS Work

This subsection briefly describes the use of MASS-DEF methodology for LWRs. Ongoing physical security research efforts as part of DOE's Light Water Reactor Sustainability (LWRS) program are focused on optimizing physical security posture at NPPs by performing reduction in number of armed guards and other physical security optimization analysis in EMRALD. The optimization framework starts with evaluating the effectiveness of the current physical security posture followed by an exaggerated analysis and staff reduction evaluation (Figure 6). The staff reduction evaluation analysis entails an iterative framework that identifies the least effective post in the plant physical security posture across an extensive set of potential attack scenarios. The framework then recommends the removal of the least effective post but only if the removal has minimal impact on the performance effectiveness of the overall security posture [11].

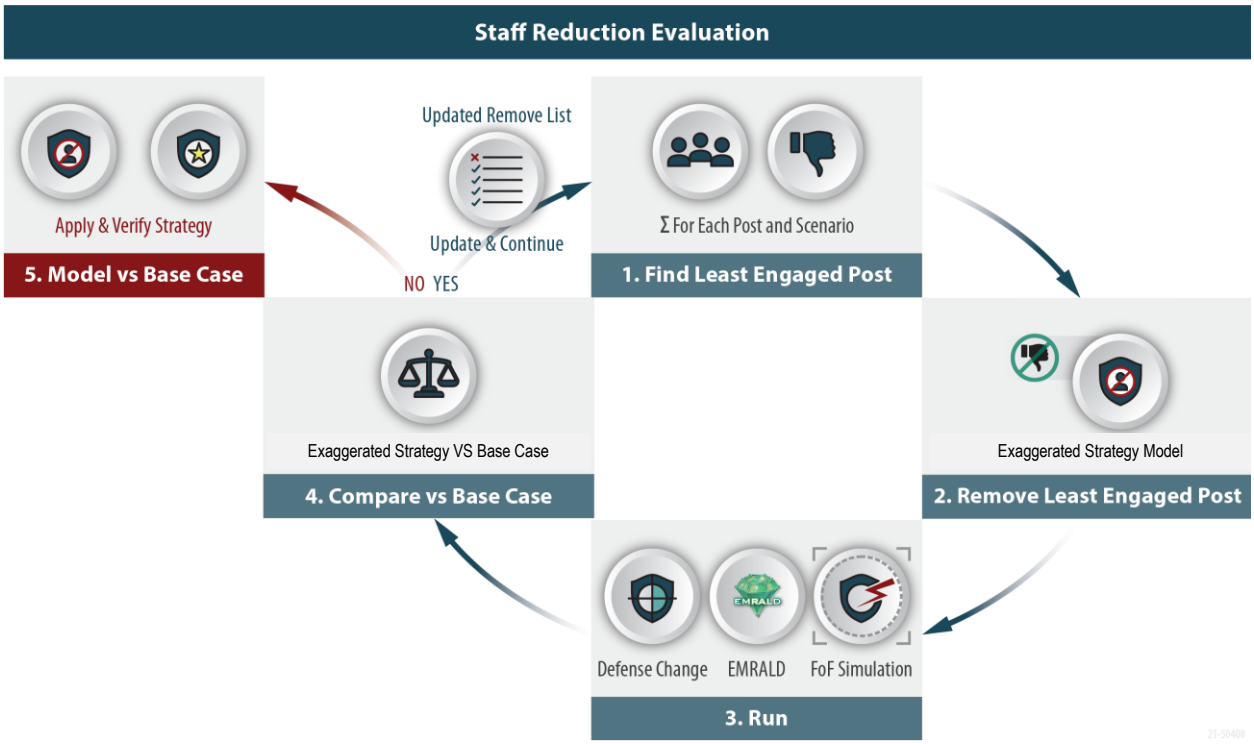


Figure 6. Process to evaluate staff reduction for strategy change.

EMRALD has also been applied for integrating FLEX-like portable equipment, such as pumps and diesel generators, and thermal-hydraulic analysis within adversarial attack scenarios aimed at causing a radiological release by sabotaging the plant's critical assets. The results of dynamic analysis in EMRALD have demonstrated that even in the extreme case of a successful adversarial attack, deploying FLEX-like portable equipment can result in a significantly high likelihood of preventing radiological release [12]. The modeling and simulation framework of integrating FLEX-like equipment with FOF models enables the NPPs to credit FLEX-like portable equipment in the plant security posture, resulting in an efficient and optimized physical security. EMRALD has been successfully applied to integrate the dynamic analysis of FLEX implementation with three FOF simulation tools SCRIBE-3D [17], AVERT[18], and Simajin [19], of which the latter two are currently being used by a majority of commercial NPPs across the nation for their FOF modeling.

3. REFERENCE SFR MODEL AND DATA

This report focuses on the physical security analysis of a generic SFR design using the dynamic methodology as described in the previous section. The following subsection describes the generic SFR facility and related data.

3.1 Plant Model and Data

The plant model used in this research is adopted from the Gen IV International Forum Example SFR (ESFR) model as described in publicly available reports [20][21][22]. The ESFR facility is a **hypothetical** Generation IV SFR model which includes four units of 800-MWth power plant, fuel cycle facilities, and a deployment scenario. The system elements in the ESFR are LWR spent-fuel storage, a co-located fuel cycle facility, ESFR spent-fuel and fresh-fuel storage cell, fuel services building (containing single fuel assembly staging/washing area and transfer tunnels for each reactor), four identical SFRs (each having an in-vessel storage basket), waste storage, LWR spent-fuel cask receiving and parking area,

excess uranium storage, and uranium container parking area. The diagram and 3d rendering of this hypothetical facility are shown in Figure 7 and Figure 8.

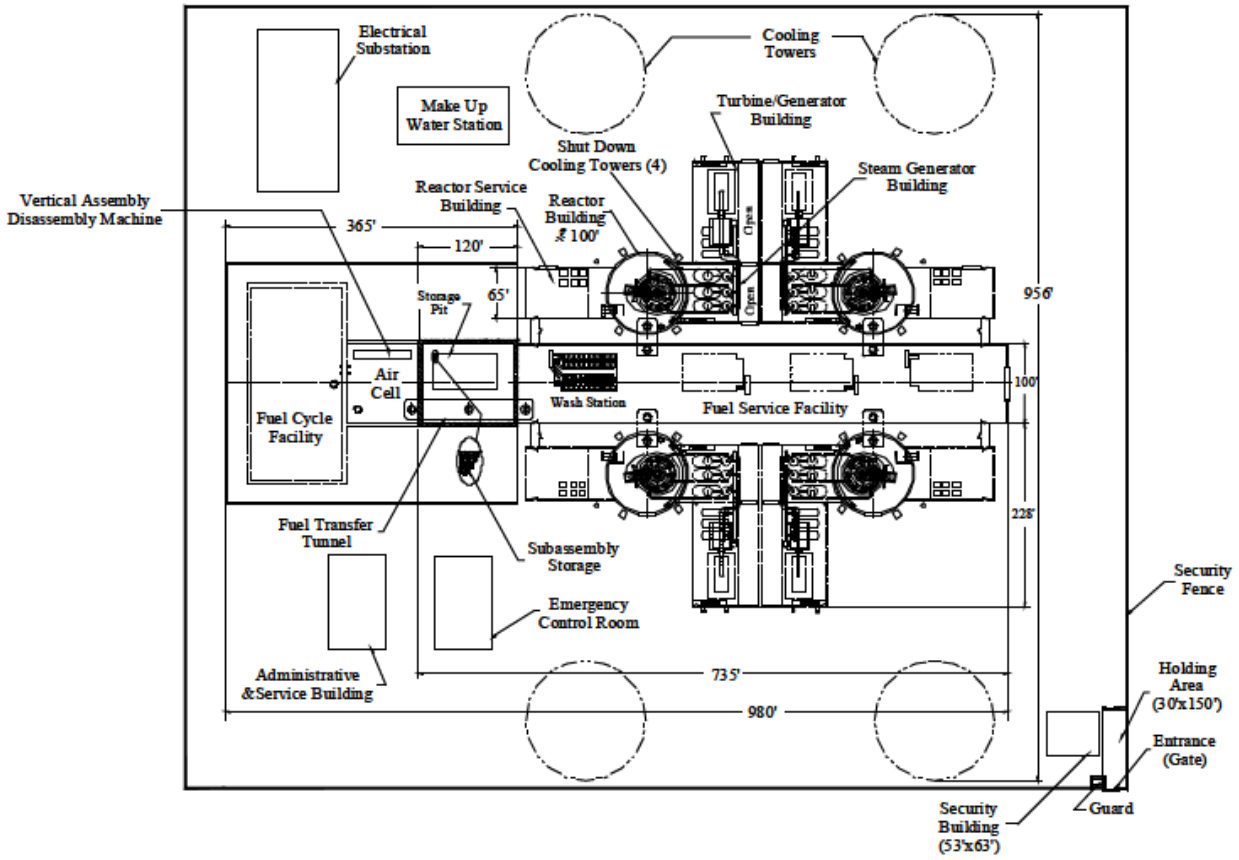


Figure 7. Diagram of ESFR facility [20].

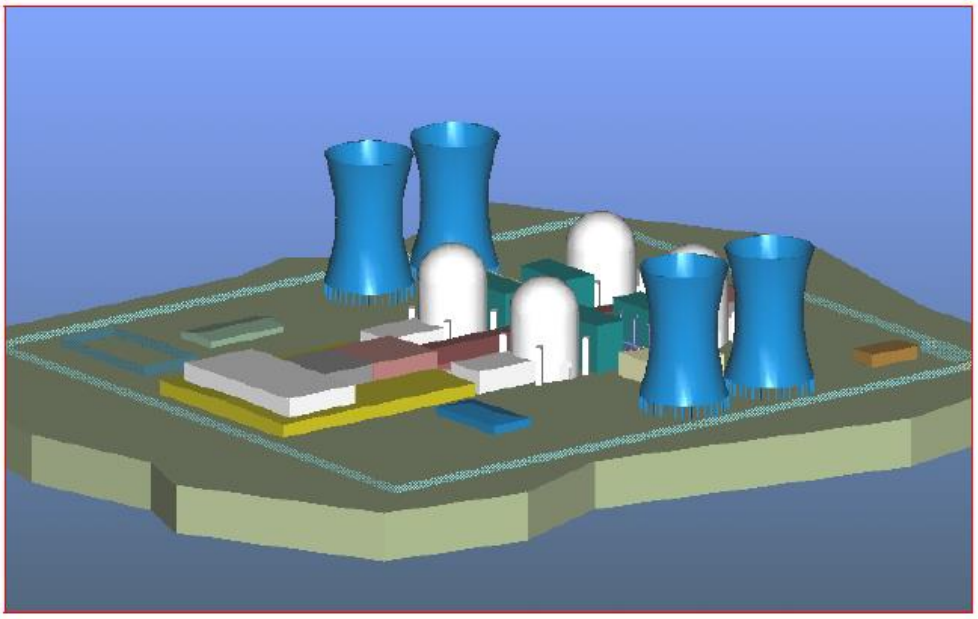


Figure 8. Site rendering for the ESFR facility [20].

3.2 Attack Scenarios

Several theft and sabotage scenarios are considered in this research. The scenarios are adapted from [20], keeping the targets, pathways delay times and detection probabilities the same while including several dynamic uncertainties in the attack and response simulations.

3.2.1 Theft Scenarios

Three theft scenarios are illustrated in Figure 9 [20]. The three targets are LWR spent fuel cask located at the LWR spent fuel cask parking area, the fuel slugs in the inert hot cell of the fuel cycle facility, and refabricated fuel assemblies in the staging and washing area.

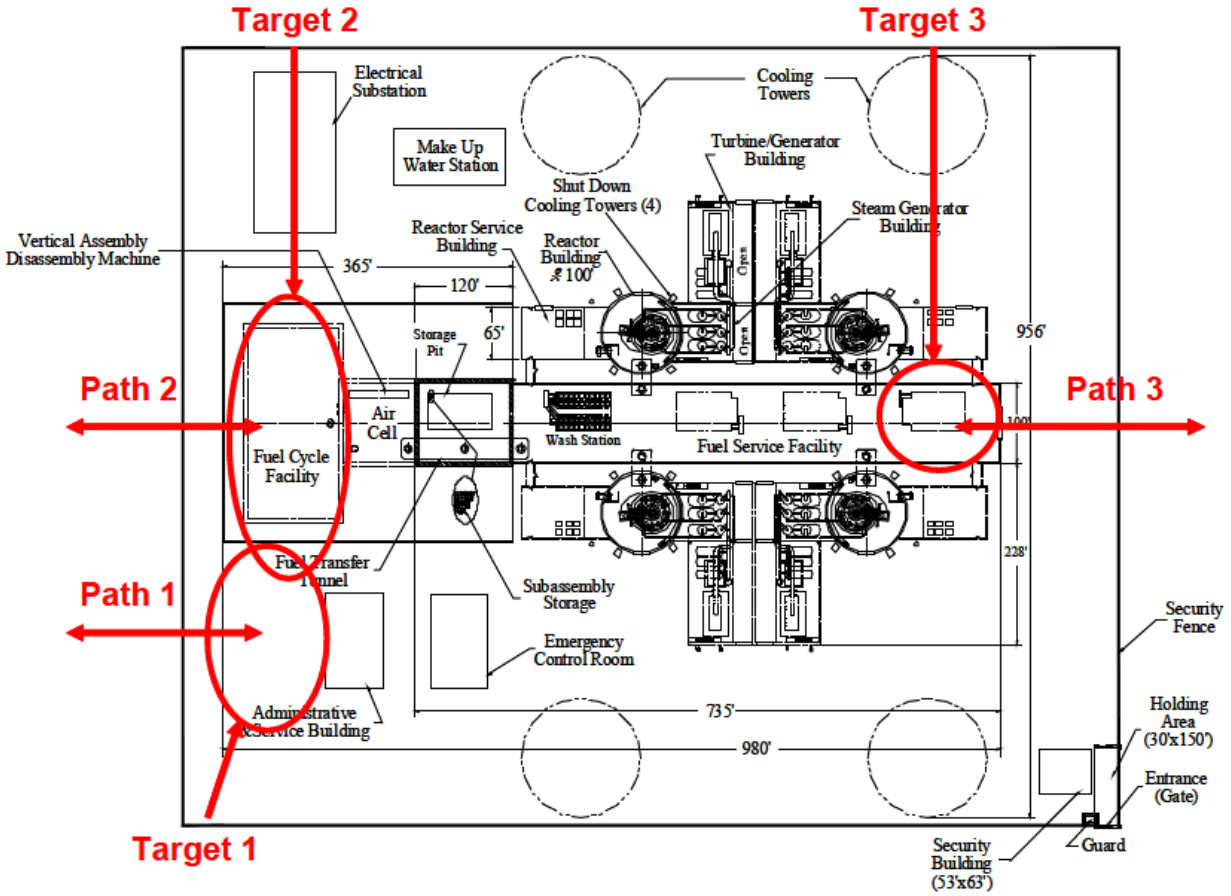


Figure 9. Theft targets and attack paths [20].

Descriptions of theft targets are summarized from [20]. The first target is the spent fuel assemblies of LWR fuel that have arrived on site and have not been unloaded from the shipping cask yet. Since these casks are large and heavy, the adversaries need to hijack the vehicle carrying these spent fuel assemblies. It is assumed that an insider assists this attack by leaving the vehicle unlocked as shown in Figure 10. Adversaries start the attack from outside, breach the plant boundary and the perimeter intrusion detection and assessment system (PIDAS), travel through the protected area to get to the spent fuel parking area, hijack the vehicle, and leave through the same path.

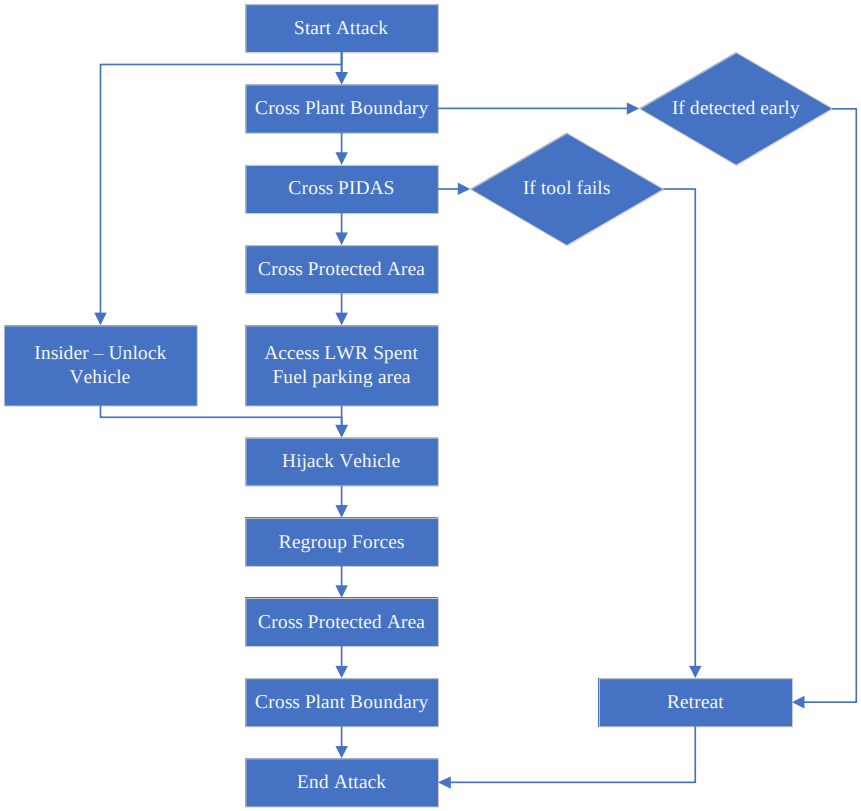


Figure 10. Theft target 1 scenario.

The second target is the reprocessed fuel slugs in an argon-inert hot cell. Uranium product and transuranic-uranium material would likely be in batch-sized slugs or pucks. The uranium, transuranic (TRU) product and fissile makeup materials are combined to form fuel slugs. The slugs are assembled into fuel pins and then into fuel elements. A theft target may include the fuel slugs or the assembled fuel elements. The attack plan is given in Figure 11.

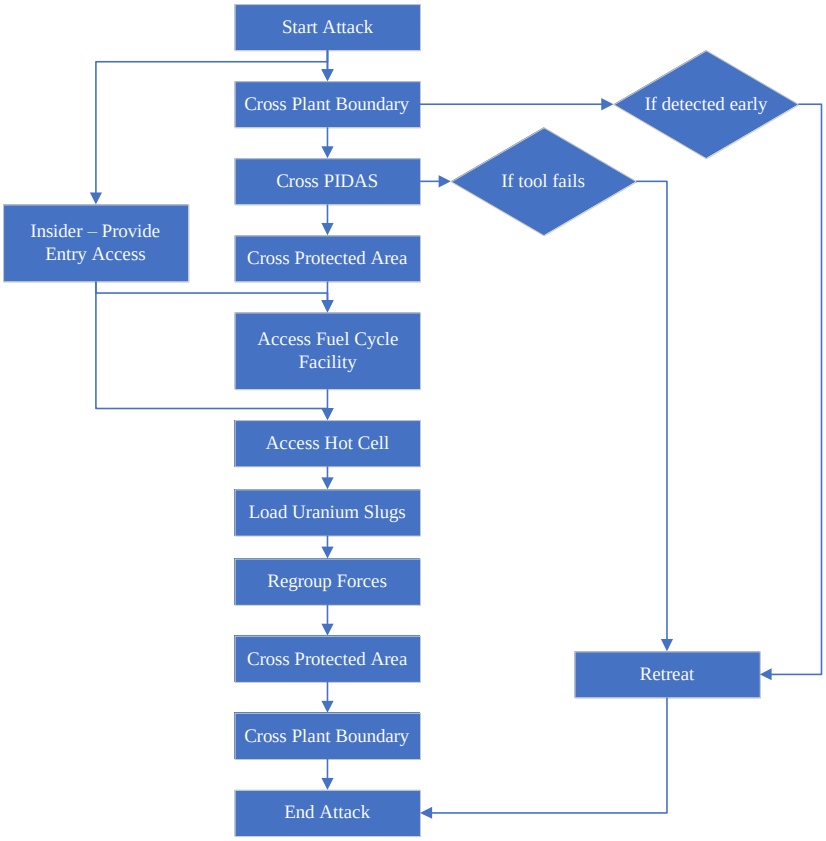


Figure 11. Theft target 2 scenario.

The third target is the full length spent fuel assemblies or refabricated assemblies in the staging and washing area. The spent assemblies are to be cleaned of external excess sodium after their removal from the adjoining reactors, while the refabricated assemblies are wetted with sodium, heated, and staged in this area for the next core load. The spent and refabricated assemblies are targets for theft. Each assembly weighs about 650 kg. The adversaries therefore need to hijack a vehicle nearby to transport these assemblies out of the facility. The attack plan is shown in Figure 12.

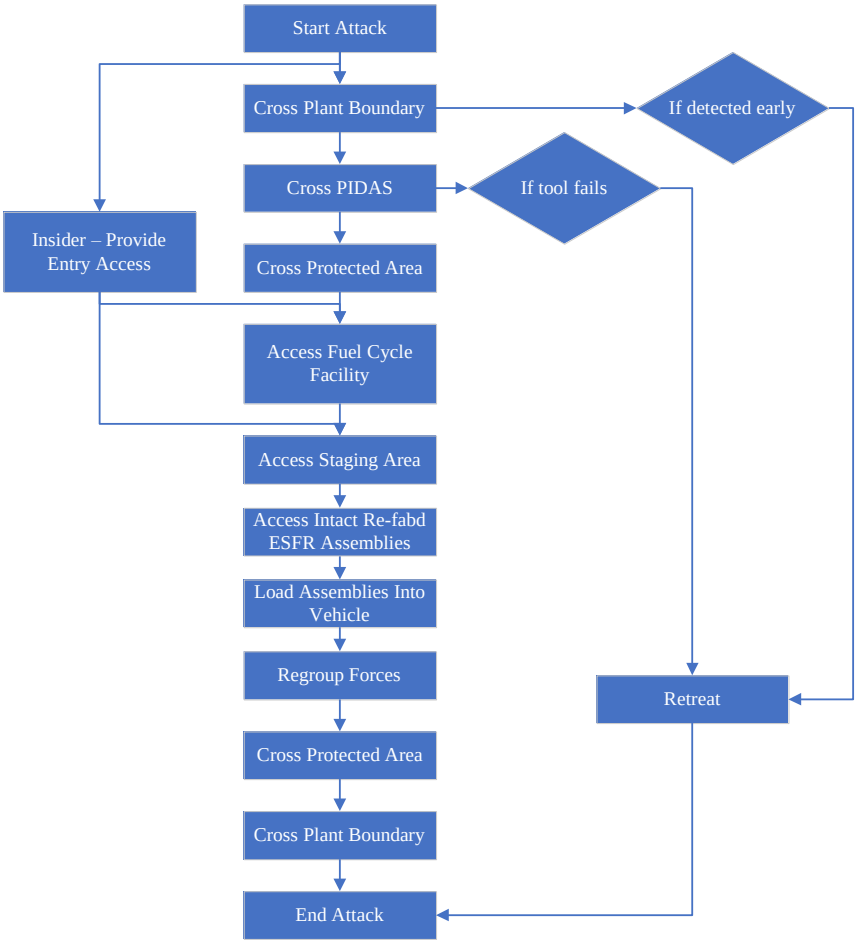


Figure 12. Theft target 3 scenario.

The detection and delay parameters for each of the actions in theft scenario 1, 2, and 3 are listed in Table 1, Table 2, and Table 3, respectively. Meanwhile, the parameters of three possible response force timings are listed in Table 4. The delay times are assumed to be normally distributed. These are the default parameters. **However, there are dynamic uncertainties introduced in this study that may vary these time parameters that do not exist in the previous studies**. To show how uncertainties are introduced, consider theft scenario 1. Adversaries begin their attack by crossing the plant boundary to get to the PIDAS. If adversaries are detected in this beginning attack stage, they will abandon their plan and retreat. If they are not detected, they will proceed to breach the PIDAS using hand tools. There is a 10% probability that the tools break or fail. If the tools break, adversaries will retreat and may consider attacking again another time. If adversaries are detected, armed responders mobilize and intercept the adversary in the planned time given in Table 4. There is a 10% probability that the responders' vehicle fails to start due to random failures. If the vehicle fails, responders' get to the destination on foot and their response time is doubled. If responders intercept adversaries, a gunfight happens for a mean time of 5 minutes and a standard deviation of 30 seconds. During the gunfight, adversaries are assumed to continue proceeding with their task. However, their task completion times are doubled. At the end of the gunfight, there is a 50%-50% chance for the responder and adversary to win the gunfight. If adversaries win, they continue with their attack plan. Additionally, there is a 50% probability for the insider assistance to fail. If the insider fails, adversaries breach barriers or unlock the vehicles using their tools, which will take them four times longer than the initial plan. These dynamic scenario uncertainties are hypothetical, yet they are introduced to illustrate the possible uncertainties to an attack plan and how it

may alter the scenario's progression and the analysis of attack outcome. **The numerical data and multipliers used in these scenario uncertainties are arbitrarily assumed and do not represent data from any actual nuclear plant.**

Table 1. Detection and delay values for the first theft scenario.

No.	Action	Detection probability	Mean delay time (seconds)	Std. deviation delay time (seconds)	Notes
1	Start attack	0	-	-	
2	Cross plant boundary	0.02	300	30	
3	Breach PIDAS	0.9	60	6	
4	Cross protected area	0.02	30	3	
5	Access LWR spent fuel area	0.02	30	3	
6	Hijack vehicle with the LWR spent fuel cask	0.95	180	18	Insider assists by leaving vehicle unlocked
7	Regroup forces	0	20	2	
8	Cross protected area	0	30	3	
9	Cross plant boundary	0	30	3	
10	End attack	0	30	3	

Table 2. Detection and delay values for the second theft scenario.

No.	Action	Detection probability	Mean delay time (seconds)	Std. deviation delay time (seconds)	Notes
1	Start attack	0	-	-	
2	Cross plant boundary	0.02	300	30	
3	Breach PIDAS	0.9	60	6	
4	Cross protected area	0.02	30	3	
5	Access fuel cycle facility	0.95	20	2	Insider assists by providing entry access
6	Access inert hot cell	0.95	180	18	Insider assists by opening equipment access port

No.	Action	Detection probability	Mean delay time (seconds)	Std. deviation delay time (seconds)	Notes
7	Load uranium product slugs into vehicle	0	120	12	
8	Regroup forces	0	20	2	
9	Cross protected area	0	30	3	
10	Cross plant boundary	0	30	3	
11	End attack	0	30	3	

Table 3. Detection and delay values for the third theft scenario.

No.	Action	Detection probability	Mean delay time (seconds)	Std. deviation delay time (seconds)	Notes
1	Start attack	0	-	-	
2	Cross plant boundary	0.02	300	30	
3	Breach PIDAS	0.9	60	6	
4	Cross protected area	0.02	30	3	
5	Access fuel cycle facility	0.95	30	3	Insider assists by providing entry access
6	Access staging / washing area	0	300	30	
7	Access intact refabricated ESFR assemblies	0	90	9	
8	Load assemblies into vehicle				
9	Regroup forces	0	20	2	
10	Cross protected area	0	30	3	
11	Cross plant boundary	0	30	3	
12	End attack	0	30	3	

Table 4. Armed responders' response times.

PPS	Mean response time (seconds)	Std. deviation of response time (seconds)
PPS A	150	15
PPS B	300	30
PPS C	600	60

3.2.2 Sabotage Scenario

The sabotage target considered in this study is the shutdown cooling system (SCS). There are four units in the facility; however, we analyze only the farthest unit from the security building for conservatism. The target and attack path are shown on Figure 13, while the attack plan is shown in Figure 14. The adversaries start the attack from offsite by crossing the plant boundary to get to the PIDAS. An insider inserts positive reactivity into the core by withdrawing the most reactive control rod, which will trigger a plant trip. The plant will trip pumps and remove decay heat using the passive cooling system. Outside adversaries breach the PIDAS and cross the protected area to disable this passive cooling system using explosives. The attack is considered successful if both the insider and outside adversaries successfully achieve their objectives.

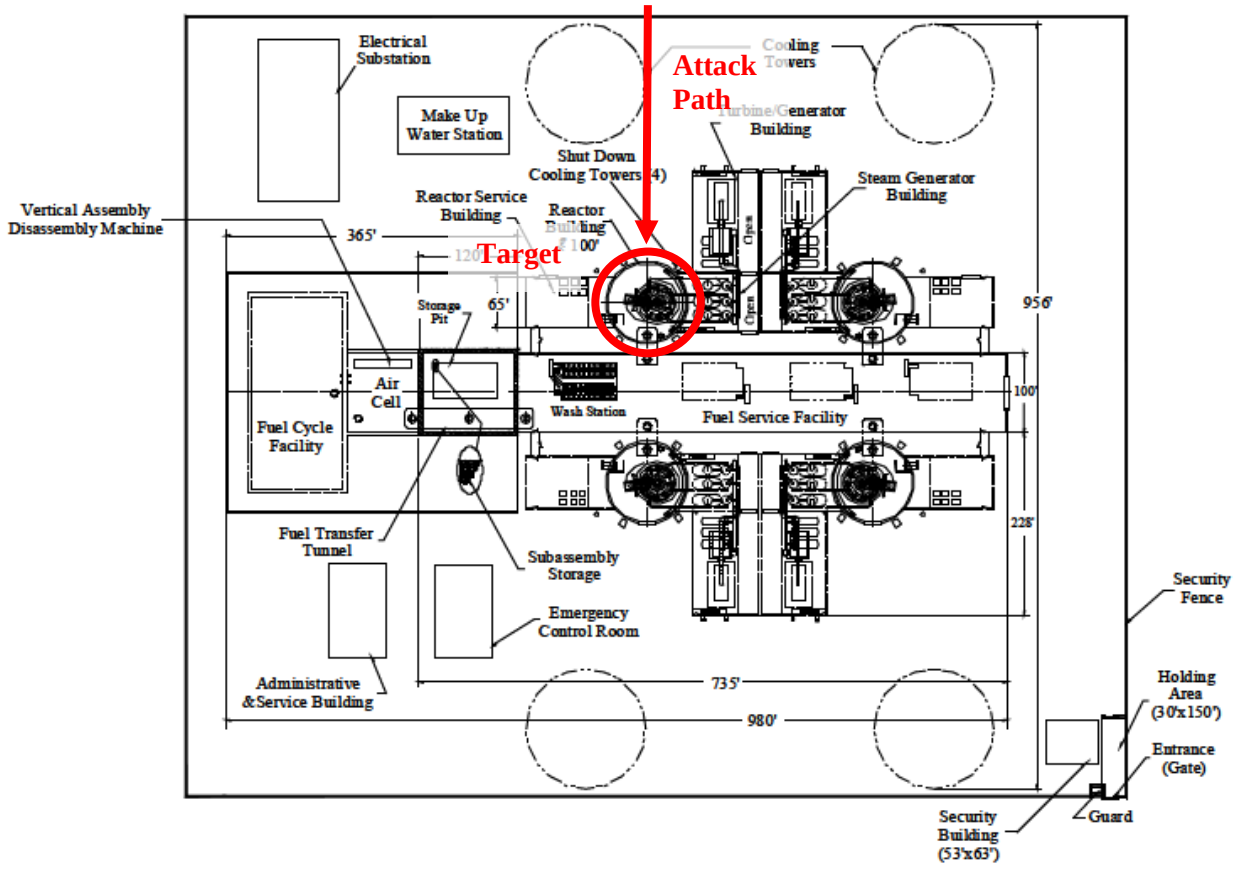


Figure 13. Sabotage target and attack path.

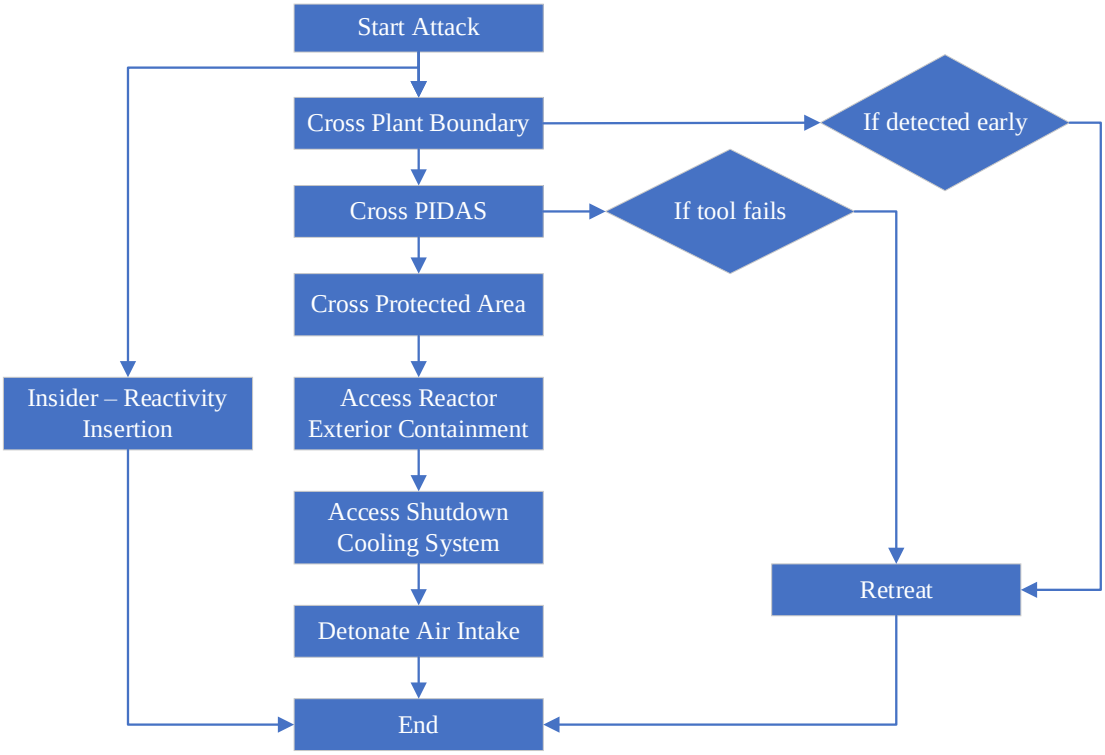


Figure 14. Sabotage attack plan.

The time delay and detection probabilities for the sabotage scenario are listed in Table 5 as adapted from [2020]. The delay and detection parameters at the plant boundary and PIDAS are taken from Table 1 to ensure consistency of the PPS parameters. The dynamic uncertainties in this scenario are similar to the ones for the theft scenarios. If adversaries are detected early in their attack or if their equipment fails early on, they will retreat to retry the attack another time. When adversaries gain access to the SCS, they set up explosives and detonate it. Adversaries' task time are doubled when they are under fire. The armed responders likewise have a 10% chance of being delayed due to random vehicle failures. The insider has a 50% chance of successfully inserting the positive reactivity. **These numbers are assumed arbitrarily and are not taken nor derived from any actual nuclear facility**.

Table 5. Detection and delay values for the sabotage scenario.

No.	Action	Detection probability	Mean delay time (seconds)	Std. deviation delay time (seconds)	Notes
1	Start attack	0	-	-	Insider inserts positive reactivity
2	Cross plant boundary	0.02	300	30	
3	Breach PIDAS	0.9	60	6	
4	Cross protected area	0.02	30	3	
5	Access reactor exterior containment	0.95	330	33	

No.	Action	Detection probability	Mean delay time (seconds)	Std. deviation delay time (seconds)	Notes
6	Access shutdown cooling system	0	30	3	
7	Detonate Air Intake	0	1200	120	
8	End attack	0	0	0	

3.3 EMRALD Models

3.3.1 Theft Scenarios

The EMRALD models for the first, second, and third theft scenarios are shown in Figure 15, Figure 16, and Figure 17 respectively. All the models begin at the StartAttack state, as identified with a green circle indicating it as the starting state of the simulation. The simulation proceeds to the CrossPlantBoundary1 State, and the SensorPlantBoundary1 action performs a sampling on the intrusion detection probability using a C# script as shown in Figure 18. This sampling script along with other detection probabilities is used in other detection actions such as SensorPidas1, Sensor_PA1, etc. It updates an internal variable named Bool_Alarm when a detection event occurs. If Bool_Alarm variable evaluates to True, the IfDetectedEarly event and the Retreat action are activated which cause the simulation to bypass the attack sequence and go to the CheckResponderData state. If adversaries do not retreat, EMRALD then samples the time it takes for them to cross the plant boundary in the PlantBoundaryCrossed event. The mean and deviation of time-based events, indicated with a Gaussian curve icon, follow the data in Table 1 to Table 3.

Adversaries proceed to breach PIDAS. The SampleToolFailure action returns whether the hand tool fails which triggers the IfToolFailed event and the Retreat action when it fails. The CrossProtectedArea1 models the adversaries crossing the protected area. The crossing time depends on whether adversaries are under fire or not. The Set_PA_Mean and Set_PA_Dev actions check the Bool_Alarm and Bool_Gunfight variables and adjust the mean and deviation times of the ProtectedAreaCrossed event and similarly for the Access_LWR_SF_ParkingArea state. In the HijackVehicle state, EMRALD samples if the adversary is successful in leaving the vehicle unlocked and unattended. The result is used to adjust the time parameters for adversaries to hijack the vehicle, as shown in Figure 19 and Figure 20. The adversaries continue with the attack plan until it reaches the EndAttack state. There are several administrative states to update and save internal EMRALD variables following the EndAttack state (i.e., CheckResponderData, WaitResponderData, SaveData, and EndSim states). The CheckResponderData state checks if the alarm has been triggered and updates the responders' time if it has. Without this variable update, the responders' time will otherwise be recorded as 0. All relevant simulation data are written to a comma-separated text file in the SafeToFile action for further statistical analysis.

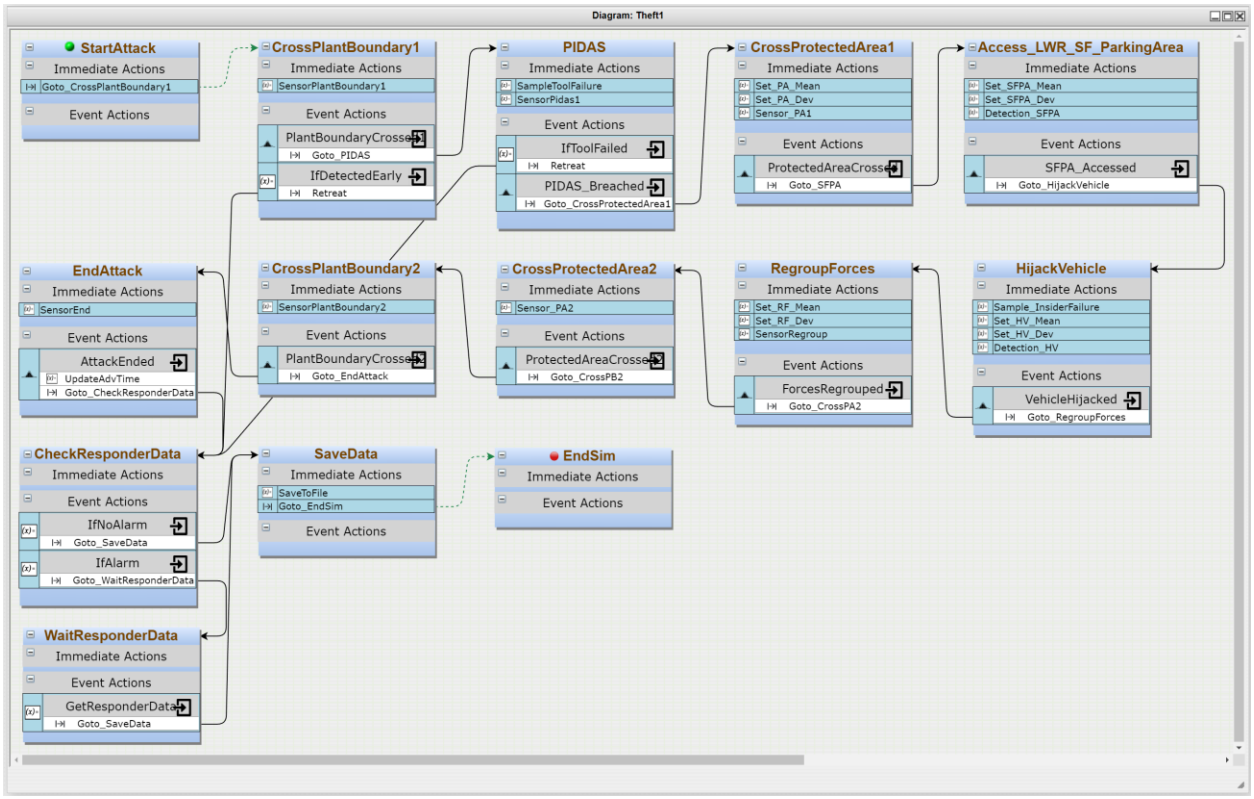


Figure 15. EMRALD model for the first theft scenario

The EMRALD models for the second and third theft scenarios follow the same design principle as the first theft scenario. They differ in terms of the sequence of states and events according to their respective attack plans. The second theft scenario for example relies on an insider to provide access to the fuel cycle facility and the inert hot cell. The insider's failure will affect the task time in the FuelCycleFacAccessed and the HotCellAccessed events.

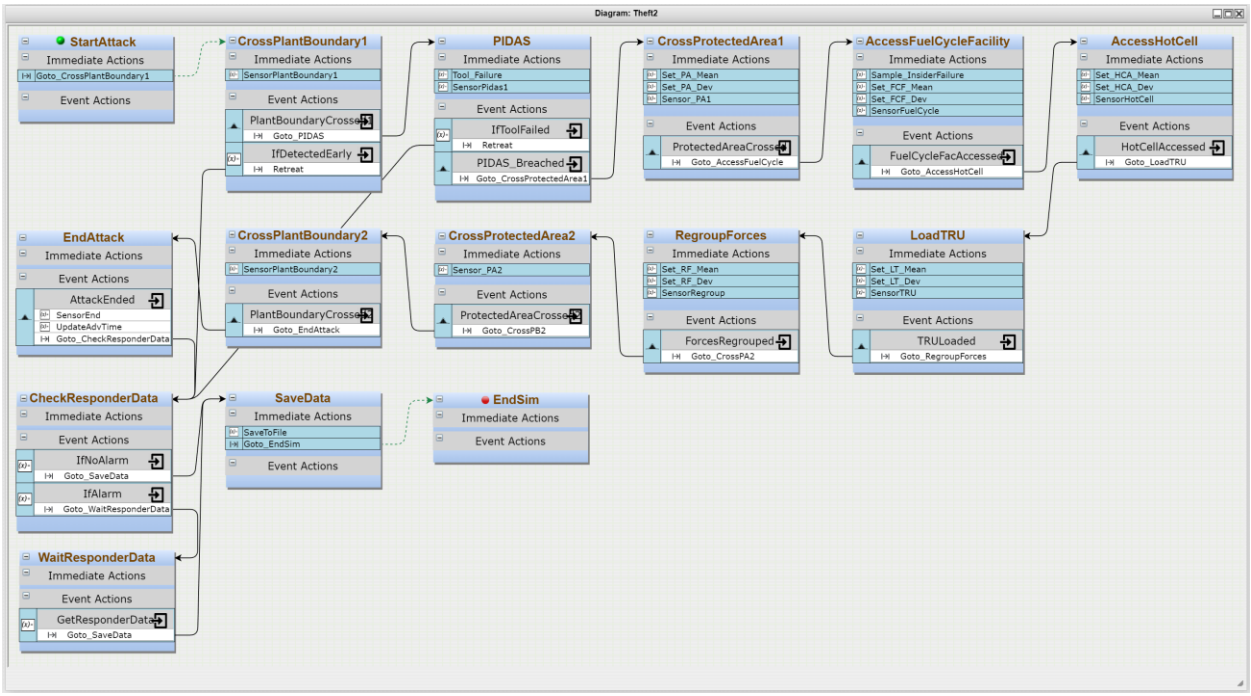


Figure 16. EMRALD model for the second theft scenario.

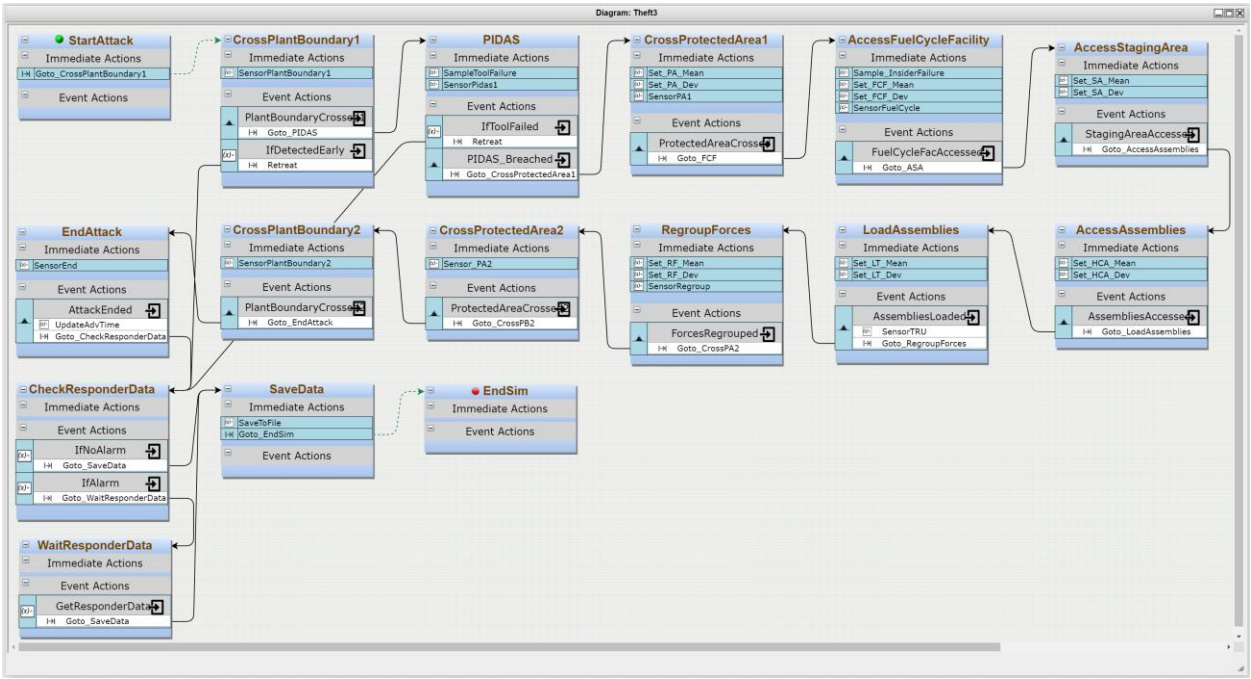


Figure 17. EMRALD model for the third theft scenario.

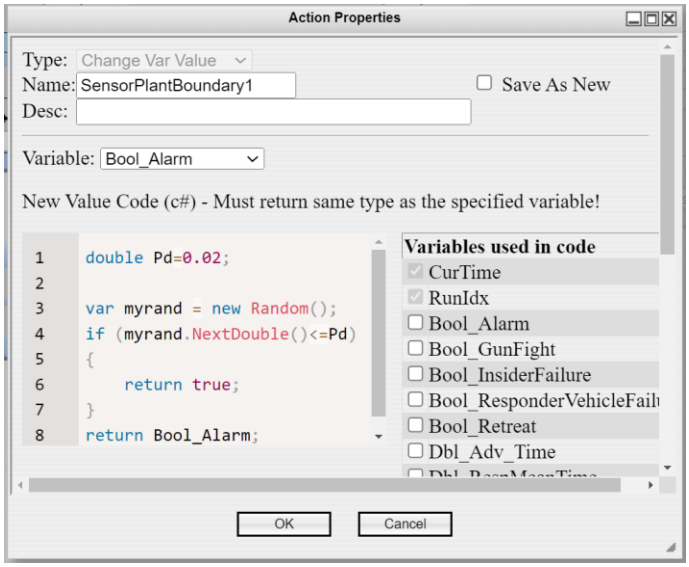


Figure 18. Example of a sensor detection script.

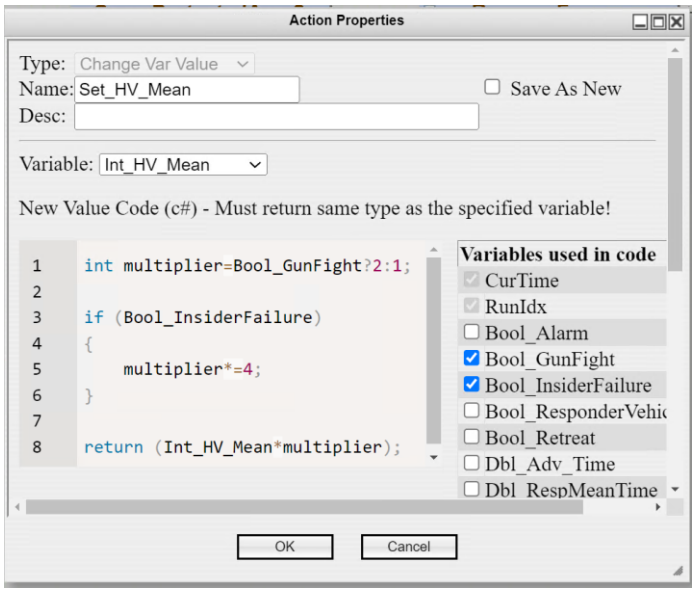


Figure 19. Example method to adjust adversary task time if they are under fire and/or if insider's action is successful.

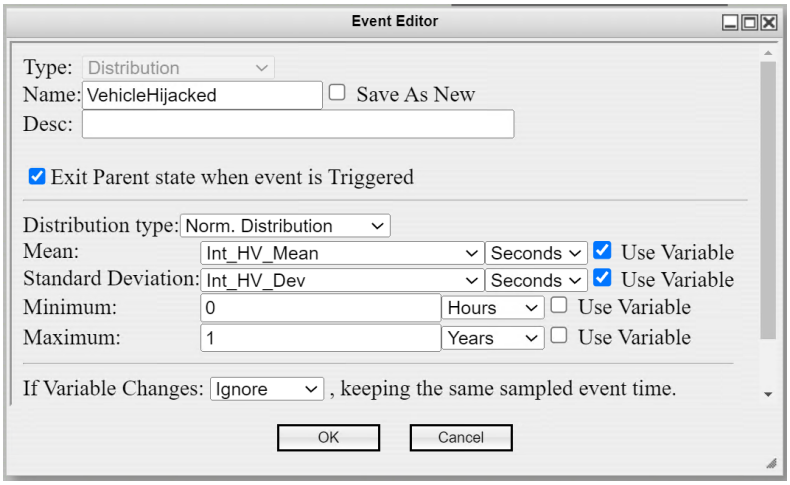


Figure 20. Example of a variable time distribution event.

The responders' diagram for all the attack scenarios is shown in Figure 21. The Responders state initiates at the start of simulation, and the IfAlarm event waits for the variable Bool_Alarm to be True. IfAlarm event activates the SendResponders state which samples the vehicle's failure and adjusts the response time accordingly. The RespondersArrived event samples the responders' travel time following a normal distribution, records the arrival time to an internal variable, and activates the CheckSituationState. If responders intercept adversaries while they are still on the site, the GunFight state becomes active and sets an internal variable Bool_GunFight to True in the SetGunFightTrue action. The GunFight event samples the shootout time from a normal distribution with a mean of 5 minutes and a standard deviation of 30 seconds. During this period, all adversary action times are doubled. Afterwards, the SetGunFightFalse action returns the Bool_GunFight variable to False, and the SampleWinTeam action samples the outcome of the GunFight event.

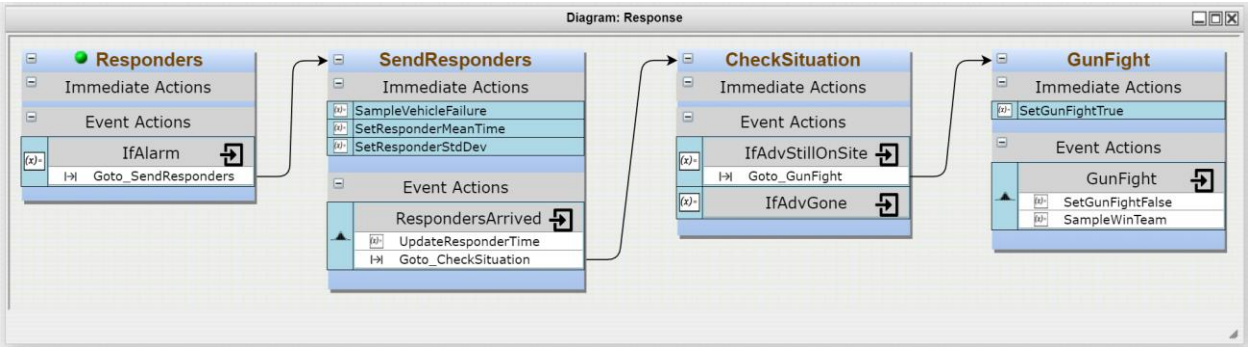


Figure 21. EMRALD model for armed responders

3.3.2 Sabotage Scenario

The EMRALD model of the sabotage scenario is shown in Figure 22. This sabotage scenario has fewer steps than the theft scenarios since it does not involve the steps to leave the site with a stolen target. The narrative for this scenario is similar to the theft scenario, with several exceptions that the insider inserts positive reactivity at the start of the attack, and the outside adversaries aim to disable the passive SCS. It is reasonably assumed that there is no communication between the insider and the outside adversaries. Therefore, the outside adversaries proceed with their plan regardless of whether the insider is successful or not.

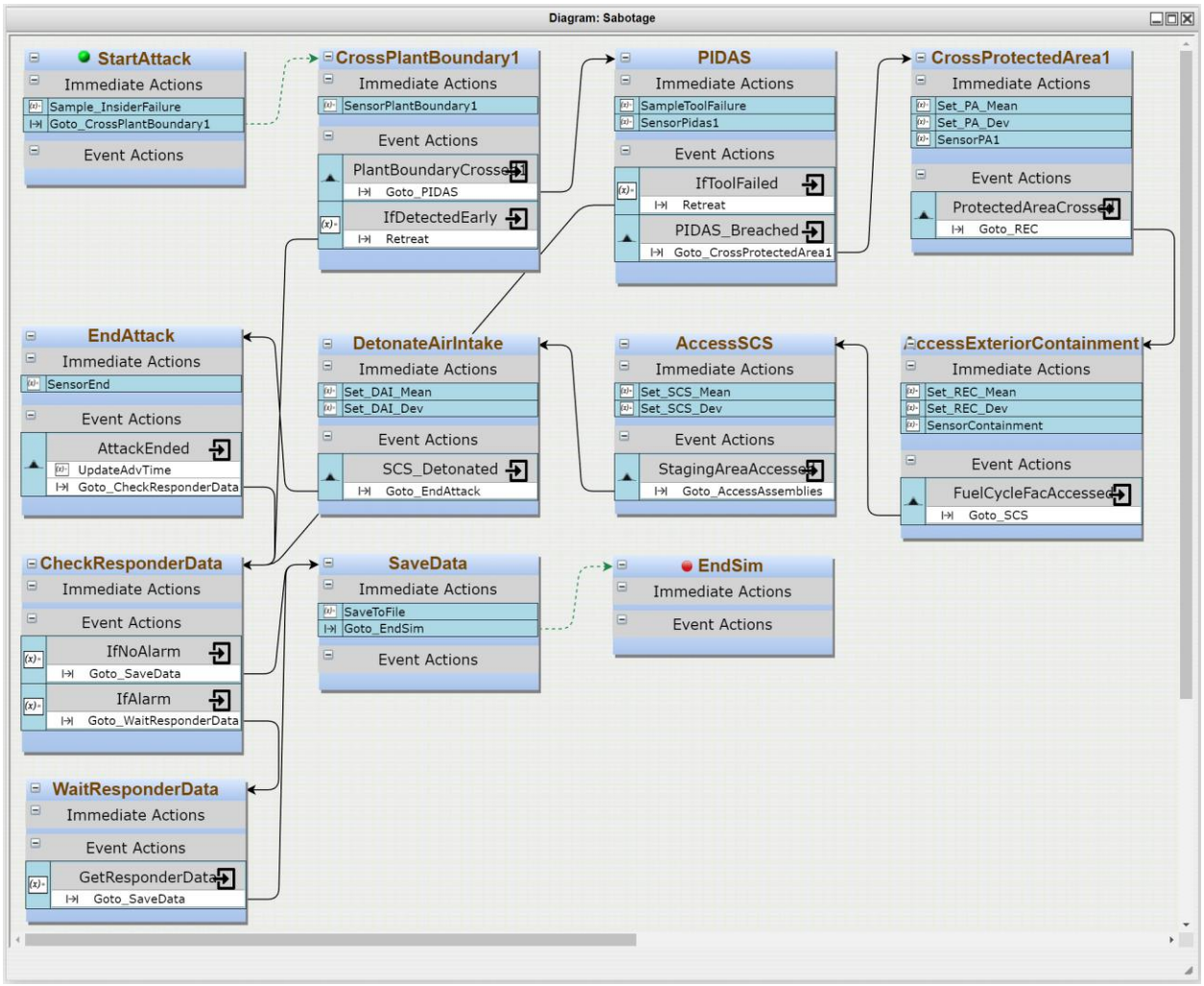


Figure 22. EMRALD model for the sabotage scenario

4. RESULTS AND DISCUSSIONS

Reference [2020] provides the numerical solutions to several attack scenarios as calculated with Estimate of Adversary Sequence Interruption (EASI) v2000. One of these solutions is selected to benchmark and/or validate EMRALD models. The selected scenario is a theft scenario for the first target (i.e., LWR spent fuel casks) using a mean response time of 5 minutes (PPS Option 2), as shown in Figure 23. The figure shows the critical detection point (CDP) located at the protected area, which implies that detection probabilities at the spent fuel parking area and on the vehicle are assumed as 0 conservatively.

	A	B	C	D	E	F	G	H	I
1									
2			***Estimate of Adversary Sequence Interruption***	Probability of Guard Communication		Force Time (in Mean	Standard Deviation		
3									
4									
5				1		300	30		
6			**Theft of Spent Fuel Shipping Casks**						
7						Delays (in Seconds):			
8		Task	Description	P(Detection)	Location	Mean:	Standard Deviation	Rt	
9		1	Initiate Attack	0	M	0	0	710	
10		2	Cross Plant Boundary	0.02	M	300	30	710	
11		3	PIDAS	0.9	M	60	6	410	
12		4	Cross Protected Area	0.02	M	30	3	350	Critical Detection Point
13		5	Access LWR SF Parking Area	0.02	M	30	3	320	
14		6	Hijack Vehicle with LWR SF Cask	0.95	M	180	18	290	
15		7	Regroup Forces	0	M	20	2	110	
16		8	Cross Protected Area	0	M	30	3	90	
17		9	Cross Plant Boundary	0	M	30	3	60	
18		10	End Attack	0	M	30	3	30	
31						710			
32			Probability of Interruption:	0.89					

Figure 23. EASI's worksheet for benchmark and validation [20].

An EMRALD model that replicates the scenario in Figure 23 is developed as shown in Figure 24. The detection probabilities within the states after the CrossProtectedArea1 state are set to 0 following the CDP designation. The dynamic uncertainties described in the previous section, such as the probabilities for tool failure, probabilities for an early retreat, failure of responder's vehicle, failure of insider's tasks, and adversaries' time adjustment during gunfights are excluded from the model for the purpose of replicating Figure 23.

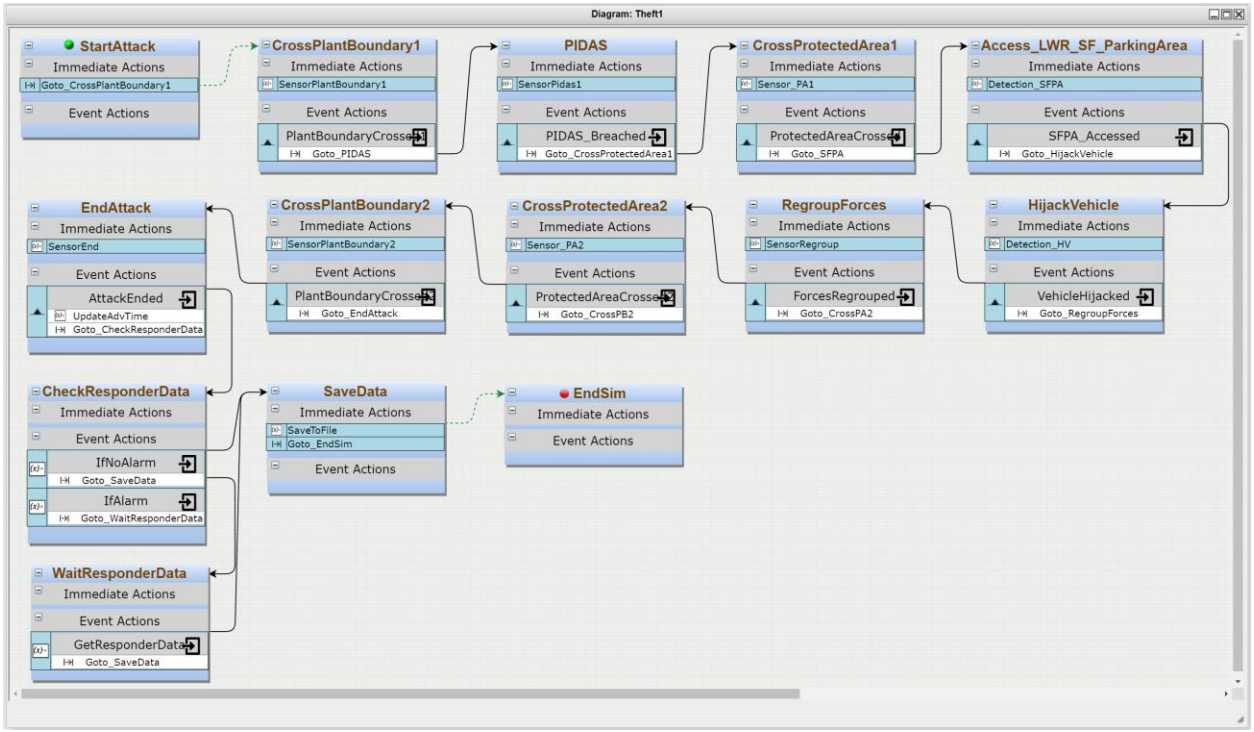


Figure 24. EMRALD model for the validation case.

The EMRALD model shown in Figure 24 was run for 10,000 cases. The timing statistics of the adversaries' mission time and responders' arrival time are plotted in Figure 25. It reveals that there is a 0.1 probability that responders are not informed of the attack. This result corresponds to the non-detection probability which equates to 1–0.904. There is also a small probability of responders intercepting adversaries around t=5 minutes, which comes from early offsite detections when adversaries are crossing the plant boundary. In most of the cases, responders intercept adversaries 2 minutes earlier than the adversaries' mission time, at around t=10 minutes. The probability of interruption was calculated as 0.9, which suggests EMRALD's agreement with EASI's calculated probability of 0.89 in Figure 23. This is a conservative result due to the absence of intrusion detection capabilities past the CDP. When CDP is removed from the model, the no-response probability decreases from 0.1 to 5E-3, and the probability of timely interruption increases from 0.89 to 0.94.

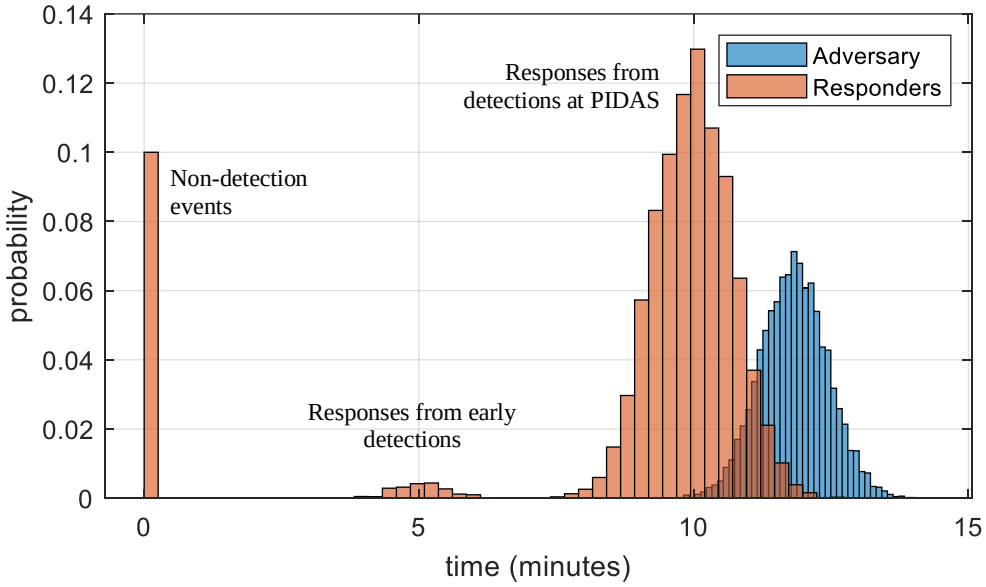


Figure 25. Timeline histogram of the validation model.

Results for the first theft scenario with PPS Option A are tabulated in Table 6. Out of 100,000 simulated cases, adversaries retreat early in 11,683 cases due to early detections and equipment failures. When adversaries continue their attack plan, they are interrupted and are neutralized 22,537 times. Adversaries complete their mission successfully in the remaining attack cases because they are not detected; they are detected but are not interrupted in time; they are interrupted in time, but they neutralize the armed responders; or they managed to leave the site on the stolen vehicle without concluding the shootout. Using values from Table 6, the probability of timely interruption within the facility is 83,392/88,317 = 0.94, which is lower than 1 as calculated in [20]. This is expected because of the difference in base assumptions. This study assumes responders' uncertainties (i.e., vehicle failure) and that early offsite detections cause adversaries to retreat before the responders arrive to interrupt them. The red-shaded cells in Table 6 indicate adversaries' success while the green-shaded cells indicate their failure. The overall probability for adversaries' success is 0.658 while the probability for their failure is 0.342.

Table 6. Results on first theft scenario with PPS Option A

<table>
<tr><td colspan="6">All attack cases: 100,000 times</td></tr>
<tr><td colspan="2">Retreat: 11,683 times</td><td colspan="4">Continue attack as planned: 88,317 times</td></tr>
<tr><td rowspan="4">Undetected: 1,003 times</td><td rowspan="4">Early detection: 10,680 times</td><td rowspan="4">Undetected: 434 times</td><td colspan="3">Detected: 87,883 times</td></tr>
<tr><td rowspan="3">Uninterrupted: 4,491 times</td><td colspan="2">Interrupted: 83,392 times</td></tr>
<tr><td colspan="2">Not neutralized: 60,855 times</td><td rowspan="3">Neutralized: 22,537 times</td></tr>
<tr><td>Left facility and complete mission before shootout is over: 38,329 times</td><td>Adversaries neutralize responders: 22,526 times</td></tr>
</table>

The timeline statistics for theft target 1 with PPS Option A are plotted in Figure 26. This timeline is more complex than Figure 25 due to the dynamic assumptions in the scenario. The probability of the adversaries' retreat is ~0.12 indicated by the blue-shaded bar at t=0, which corresponds to the retreat count in Table 6. Adversaries' time distribution between 10–15 minutes is the expected attack plan's completion time, while the distribution around 20–25 minutes might originate from the time delay due to the gunfight with armed responders. The wide distribution from t=27 minutes to t=37 minutes might be caused by the delay from gunfight and the delay caused by the insider's failure. As for the armed responders, the time at t=0 reflects the probability of non-detection. The time distribution up to t=5 minutes indicates the response due to early detections at the plant boundary. Most of the time, responders arrive between 5 to 10 minutes as a result of the high detection probability at the PIDAS. Sometimes they are delayed up to 10 minutes due to vehicle failure events.

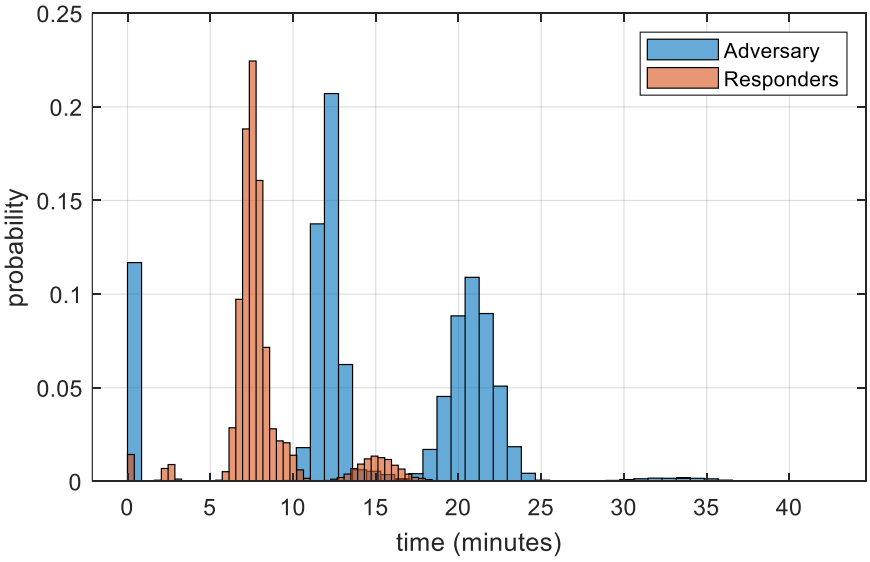


Figure 26. Timeline histogram for the first theft scenario with PPS Option A.

Detailed results and timelines for other attack scenarios are listed in Appendix A. The histogram of adversaries' mission time in these scenarios generally exhibit distinct peaks as identified in Figure 26. Similarly with the histogram for responders' arrival time, except that the peak response time for early detection events tend to coincide with the response time due to PIDAS detection events in PPS Option C. This is because the time intervals between offsite detection and PIDAS detection timings are

indistinguishable when compared to the long response time in PPS Option C. For the scenario of stealing target 2 with PPS Option C, the probability of interruption is very low at 0.01. This is because the responders arrive when the adversaries almost or already have left the site with the stolen material.

A summary of results from all the attack scenarios in this study is listed in Table 7. The theft targets sorted from the most to least vulnerable are target 2, target 1, and target 3, which correspond to their physical distance from armed responders and the complexity of the attack plan. The probability of adversaries' retreats due to early detection and early tool failure events serves as the baseline value for the probability of effectiveness (P_E), as seen in the theft target 2 scenario with PPS Option C where the P_E is higher than the probability of interruption (P_I). The 0.12 P_E value might result from the cumulative probability of early detection (0.02) and equipment failure (0.1). The sabotage target is quite well protected since it is close to the responders, and the time required to complete the attack is quite long, such that there is only a slight reduction in the P_E value when the responders are delayed.

Table 7 lists the P_I values calculated with EASI in [20] for comparison. The reference does not provide P_E values. It can be generally observed that P_I values from the dynamic methodology introduce more realism. In cases where the reference P_I equals 1 indicating adversaries are always interrupted, the P_I from the dynamic methodology is slightly less than 1 indicating that there is a low probability that adversaries are not interrupted. In cases where the reference P_I equals 0 indicating adversaries are never interrupted, the P_I from the dynamic methodology shows there is a low probability (0.01) that adversaries can be interrupted before they complete their mission.

Table 7. Summary of results.

Attack scenario	PPS	Static probability of interruption (P_I) calculated with EASI [2020]	Dynamic probability of interruption (P_I) calculated with EMRALD	Probability of effectiveness (P_E) calculated with EMRALD
Theft target 1	A	1	0.94	0.34
	B	0.89	0.87	0.27
	C	0.01	0.45	0.18
Theft target 2	A	1	0.90	0.29
	B	0.46	0.85	0.13
	C	0	0.01	0.12
Theft target 3	A	0.99	0.99	0.50
	B	0.99	0.97	0.47
	C	0.99	0.89	0.43
Sabotage	A	1	~1	0.75
	B	1	0.99	0.75
	C	1	0.90	0.72

Note that these results are obtained from a hypothetical facility with basic, non-exhaustive assumptions on the dynamics of the attack and response scenarios and by using arbitrarily assumed

numerical parameters. Therefore, the results do not inform security postures on any actual nuclear facility. Utilities may adopt the methodology and modify the scenarios, assumptions, parameters, and EMRALD models following their plant designs to obtain more realistic assessments.

Recommendations to improve the security posture follow the general guidelines of PPS design and evaluation methodology [23]. Improvements can be done by enhancing the intrusion detection system to detect adversaries early in their advance and to add barriers after detection points to delay them sufficiently and provide more time for the response force's arrival. Guard posts may also be situated at strategic locations within the site to intercept adversaries before the main response team arrives. These guard posts may be more beneficial on multi-unit facilities such as ESFR but may not be desirable on smaller single unit sites. Upgrades on armed responders' equipment may also be considered to reduce their travel time and to increase the probability of neutralizing the adversaries.

5. SUMMARY AND FUTURE WORK

This report presents the regulatory requirements and directions on the physical security of advanced nuclear reactors in the United States. Presently, a rule is being proposed that allows for a performance-based analysis on the physical security posture of advanced reactors. In determining the physical security requirements for an advanced reactor, new tools may be desired to conduct a performance-based analysis. These tools should incorporate dynamic analysis methods to provide as much realism as possible. In comparison, the security requirements for existing LWRs are much more prescriptive, and the analysis conducted to establish the required physical security strategies were more easily performed with static analysis. To achieve the cost goals that advanced reactors require for adoption, the nuclear security force required should not be excessive. Dynamic physical security analysis methods and tools have been developed by the DOE LWRS program. This report details how the dynamic risk analysis tools developed in the LWRS program using the dynamic risk modeling tool, EMRALD, may be adapted for use in analyzing the physical security designs for advanced reactors accounting for variable performance-based requirements. This report provides an example analysis of a hypothetical SFR. Future work in this area will create additional models that can be adapted for any advanced reactor concept and use various security features to create a physical security system that provides adequate protection from radiological theft and sabotage.

6. REFERENCES

1. NEI, 2019, "18-04 Rev. 1: Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development," ML19241A472, Nuclear Energy Institute, https://www.nrc.gov/docs/ML1924/ML19241A472.pdf.
2. U.S. NRC, 2007, "Part 50—Domestic Licensing of Production And Utilization Facilities," U.S. Nuclear Regulatory Commission, https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/full-text.html.
3. U.S. NRC, 2007, "Part 52—Licenses, Certifications, And Approvals for Nuclear Power Plants," U.S. Nuclear Regulatory Commission, https://www.nrc.gov/reading-rm/doc-collections/cfr/part052/full-text.html.
4. U.S. NRC, 2020, "Regulatory Guide 1.233 Revision 0: Guidance for A Technology-Inclusive, Risk-Informed, And Performance-Based Methodology To Inform The Licensing Basis And Content Of Applications For Licenses, Certifications, And Approvals For Non-Light-Water Reactors," U.S. Nuclear Regulatory Commission, https://www.nrc.gov/docs/ML2009/ML20091L698.pdf.
5. U.S. NRC, 2021, "10 CFR Part 53: Risk-Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors," U.S. Nuclear Regulatory Commission, https://www.regulations.gov/document/NRC-2019-0062-0159.
6. NEI, 2016, "Proposed Physical Security Requirements For Advanced Reactor Technologies," ML17026A474, Nuclear Energy Institute, https://www.nrc.gov/docs/ML1702/ML17026A474.pdf.
7. U.S. NRC, 2012, "73.55 Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage", U.S. Nuclear Regulatory Commission, https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0055.html.
8. U.S. NRC, 2018, "SECY-18-0076: Options and Recommendation for Physical Security for Advanced Reactors," ML18170A051, U.S. Nuclear Regulatory Commission, https://www.nrc.gov/docs/ML1817/ML18170A051.html
9. U.S. NRC, 2019, "Physical Security for Advanced Reactors; Request for Comment on Regulatory Basis," U.S. Nuclear Regulatory Commission, https://www.regulations.gov/document/NRC-2017-0227-0001.
10. U.S. NRC, 2022, "SECY-22-0072: Proposed Rule: Alternative Physical Security Requirements for Advanced Reactors (RIN 3150-AK19)," U.S. Nuclear Regulatory Commission, https://www.nrc.gov/docs/ML2133/ML21334A003.html.
11. 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
12. Christian, R., V. Yadav, S. R. Prescott, S. W. St. Germain, and J. Weathersby, 2020, "Methodology and Application of Physical Security Effectiveness Based on Dynamic Force-on-Force Modeling," INL/EXT-20-59891, Idaho National Laboratory.
13. U.S. NRC, 2019, “50.34 Contents of applications; technical information,” U.S. Nuclear Regulatory Commission.
14. U.S. NRC, 2019, “52.79 Contents of applications; technical information in final safety analysis report,” U.S. Nuclear Regulatory Commission.
15. Prescott, S., C. Smith, and L. Vang, 2018, “EMRALD, Dynamic PRA for the Traditional Modeler,” Presented at Proceeding of PSAM 14, Los Angeles, CA, September 2018.
16. Pidd, M., 1995, “Object-Orientation, Discrete Simulation and the Three-Phase Approach,” *The Journal of the Operational Research Society* 46 (3): 362, http://doi.org/10.2307/2584330.
17. Noel, T., T. Le, E. Parks, and S. Stromberg, 2018, “SCRIBE 3D-Tabletop Recorder v. 1.1”, U.S. Department of Energy.

18. ARES, 2020, “AVERT Physical Security,” ARES Security Corporation, Accessed February 13, 2023, https://aressecuritycorp.com/software/avert-suite.
19. Rhinocorps, “Simajin: Simulation Application Suite”, Rhinocorps Ltd. Co., Accessed February 13, 2023, https://www.rhinocorps.com/products/simulation-application-suite.
20. Gen IV International Forum Proliferation Resistance and Physical Protection Evaluation Methodology Working Group, 2009, “GIF/PRPPWG/2009/002: PR&PP Evaluation: ESFR Full System Case Study Final Report.”, https://gif.jaea.go.jp/methodology/prppwg/prpp_csreport_and_appendices_2009_10-29.pdf.
21. Gen IV International Forum, 2021, “GIF/PRPPWG/2021/003: GIF Sodium-Cooled Fast Reactor Proliferation Resistance and Physical Protection White Paper.”, https://www.gen-4.org/gif/upload/docs/application/pdf/2021-11/sfr_prpp_white_paper_2021_final_18102021v8_2021-11-10_13-50-7_552.pdf.
22. Hill, R. N., I. Therios, B. Cipiti, and H. D. Kim, 2020, “Sodium-cooled Fast Reactor (SFR) Proliferation Resistance and Physical Protection White Paper,” SAND2020-12214R, Sandia National Laboratory, https://www.osti.gov/servlets/purl/1710232.
23. Garcia, M. L., 2001, “The Design and Evaluation of Physical Protection Systems,” Butterworth-Heinemann.

Page intentionally left blank

Appendix A
Detailed Results for Each Attack Scenario

Page intentionally left blank

Appendix A
Detailed Results for Each Attack Scenario

Results from the theft and sabotage scenarios are given in this appendix.

Table A-1. Theft target 1 PPS B.

<table>
<tr><td colspan="7">All attack cases: 100,000 times. P_E = 0.27</td></tr>
<tr><td colspan="2">Retreat: 11,849 times</td><td colspan="5">Continue attack as planned: 88,151 times</td></tr>
<tr><td rowspan="4">Undetected: 966 times</td><td rowspan="4">Early detection: 10,883 times</td><td rowspan="4">Undetected: 433 times</td><td colspan="4">Detected: 87,718 times</td></tr>
<tr><td rowspan="3">Uninterrupted: 10,852 times</td><td colspan="3">Interrupted: 76,866 times</td></tr>
<tr><td colspan="2">Not neutralized: 61,837 times</td><td rowspan="2">Neutralized: 15,029 times</td></tr>
<tr><td>Left facility and complete mission before shootout is over: 46,781 times</td><td>Adversaries neutralize responders: 15,056 times</td></tr>
</table>

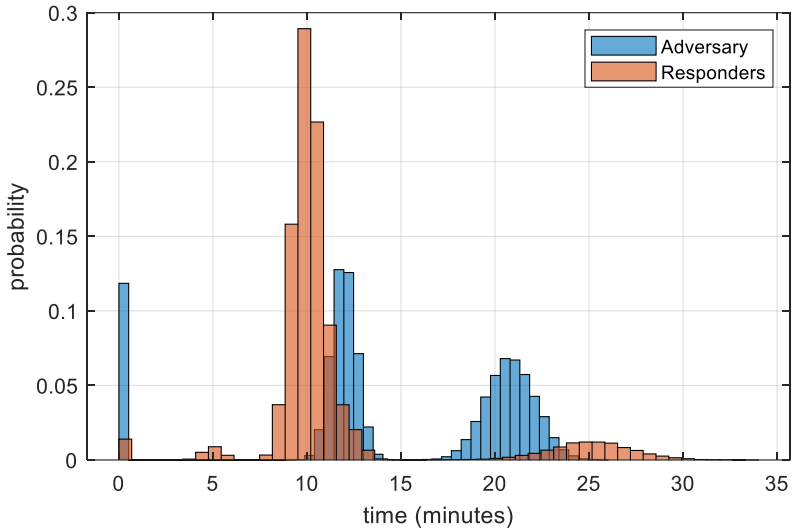


Figure A-1. Timeline histogram for theft target 1 PPS B.

Table A-2. Theft target 1 PPS C.

<table>
<tr><td colspan="6">All attack cases: 100,000 times. P_E = 0.18</td></tr>
<tr><td colspan="2">Retreat: 11,750 times</td><td colspan="4">Continue attack as planned: 88,250 times</td></tr>
<tr><td>Undetected: 1,009 times</td><td>Early detection: 10,741 times</td><td>Undetected: 35 times</td><td colspan="3">Detected: 88,215 times</td></tr>
<tr><td rowspan="3"></td><td rowspan="3"></td><td rowspan="3"></td><td>Uninterrupted: 48,330 times</td><td colspan="2">Interrupted: 39,885 times</td></tr>
<tr><td rowspan="2"></td><td>Not neutralized: 33,996 times</td><td rowspan="2">Neutralized: 5,889 times</td></tr>
<tr><td>Left facility and complete mission before shootout is over: 28,166 times</td><td>Adversaries neutralize responders: 5,830 times</td></tr>
</table>

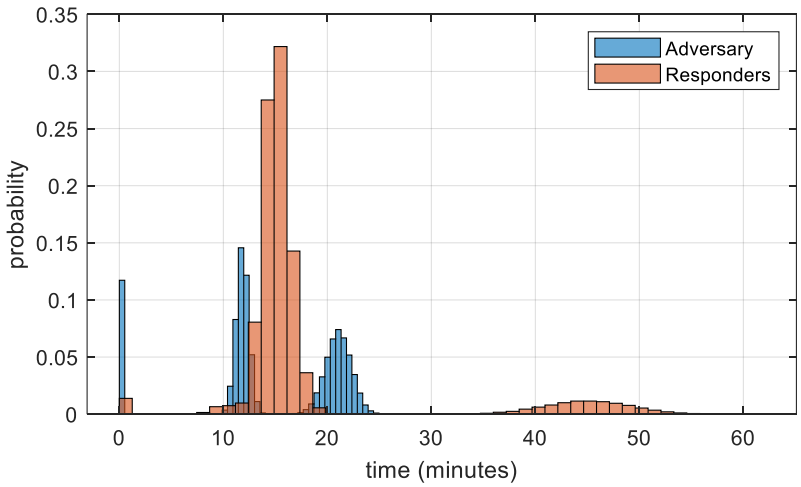


Figure A-2. Timeline histogram for theft target 1 PPS C.

Table A-3. Theft target 2 PPS A.

<table>
<tr><td colspan="6">All attack cases: 100,000 times. P_E = 0.29</td></tr>
<tr><td colspan="2">Retreat: 11,935 times</td><td colspan="4">Continue attack as planned: 88,065 times</td></tr>
<tr><td>Undetected: 1,019 times</td><td>Early detection: 10,916 times</td><td>Undetected: 21 times</td><td colspan="3">Detected: 88,044 times</td></tr>
<tr><td rowspan="3"></td><td rowspan="3"></td><td rowspan="3"></td><td>Uninterrupted: 8,631 times</td><td colspan="2">Interrupted: 79,413 times</td></tr>
<tr><td rowspan="2"></td><td colspan="2">Not neutralized: 62339 times</td><td rowspan="2">Neutralized: 17,074 times</td></tr>
<tr><td>Left facility and complete mission before shootout is over: 45,212 times</td><td>Adversaries neutralize responders: 17,127 times</td></tr>
</table>

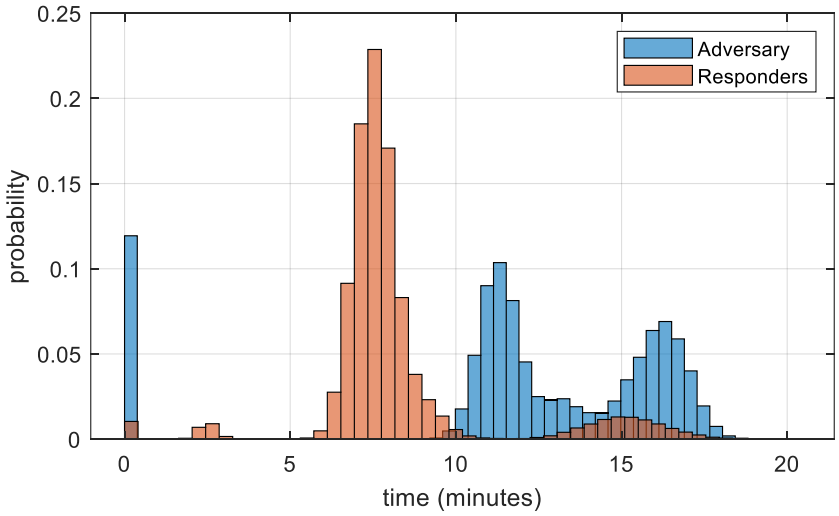


Figure A-3. Timeline histogram for theft target 2 PPS A.

Table A-4. Theft target 2 PPS B.

<table>
<tr><td colspan="7">All attack cases: 100,000 times. P_E = 0.13</td></tr>
<tr><td colspan="2">Retreat: 11,734 times</td><td colspan="5">Continue attack as planned: 88,266 times</td></tr>
<tr><td rowspan="4">Undetected: 991 times</td><td rowspan="4">Early detection: 10,743 times</td><td rowspan="4">Undetected: 19 times</td><td colspan="4">Detected: 88,247 times</td></tr>
<tr><td rowspan="3">Uninterrupted: 13,662 times</td><td colspan="3">Interrupted: 74,585 times</td></tr>
<tr><td colspan="2">Not neutralized: 73,677 times</td><td rowspan="2">Neutralized: 908 times</td></tr>
<tr><td>Left facility and complete mission before shootout is over: 72,765 times</td><td>Adversaries neutralize responders: 912 times</td></tr>
</table>

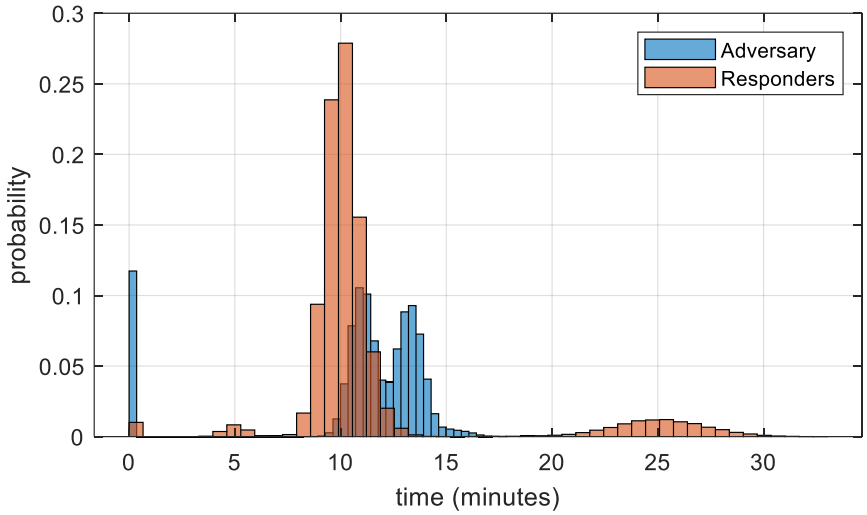


Figure A-4. Timeline histogram for theft target 2 PPS B.

Table A-5. Theft target 2 PPS C.

<table>
<tr><td colspan="5">All attack cases: 100,000 times. P_E = 0.13</td></tr>
<tr><td colspan="2">Retreat: 11979 times</td><td colspan="3">Continue attack as planned: 88,021 times</td></tr>
<tr><td rowspan="4">Undetected: 1,014 times</td><td rowspan="4">Early detection: 10,965 times</td><td rowspan="4">Undetected: 18 times</td><td colspan="2">Detected: 88,003 times</td></tr>
<tr><td rowspan="3">Uninterrupted: 87,016 times</td><td>Interrupted: 987 times</td></tr>
<tr><td>Not neutralized: 987 times</td></tr>
<tr><td>Left facility and complete mission before shootout is over: 987 times</td></tr>
</table>

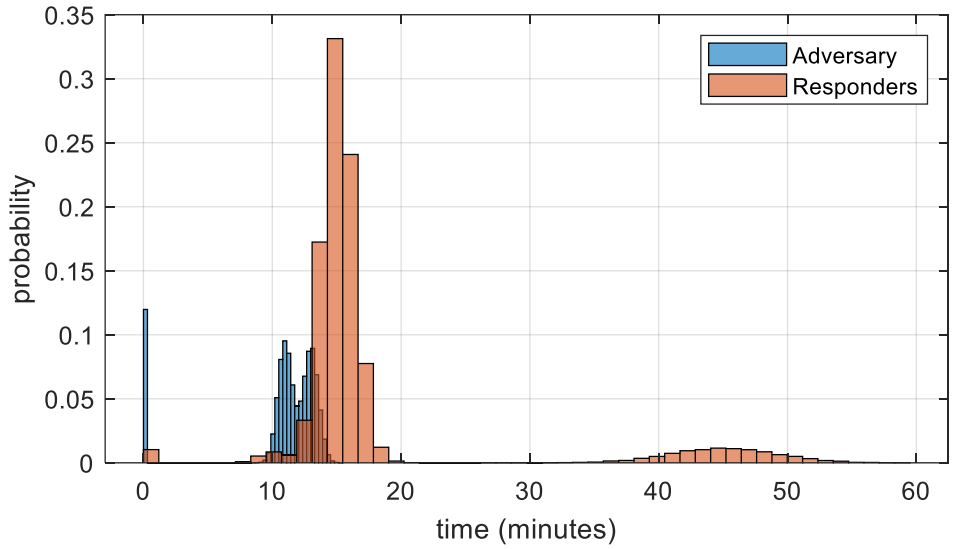


Figure A-5. Timeline histogram for theft target 2 PPS C.

Table A-6. Theft target 3 PPS A.

<table>
<tr><td colspan="6">All attack cases: 100,000 times. P_E = 0.50</td></tr>
<tr><td colspan="2">Retreat: 11,867 times</td><td colspan="4">Continue attack as planned: 88,133 times</td></tr>
<tr><td rowspan="4">Undetected: 998 times</td><td rowspan="4">Early detection: 10,869 times</td><td rowspan="4">Undetected: 446 times</td><td colspan="3">Detected: 87,687 times</td></tr>
<tr><td colspan="3">Interrupted: 87,687 times</td></tr>
<tr><td colspan="2">Not neutralized: 49,215 times</td><td rowspan="2">Neutralized: 38,472 times</td></tr>
<tr><td>Left facility and complete mission before shootout is over: 10,827 times</td><td>Adversaries neutralize responders: 38,388 times</td></tr>
</table>

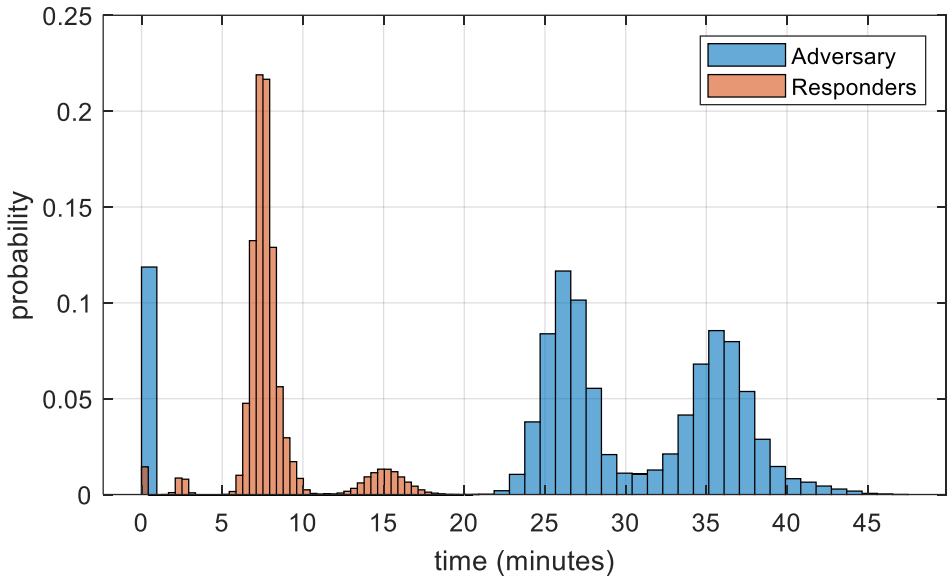


Figure A-6. Timeline histogram for theft target 3 PPS A.

Table A-7. Theft target 3 PPS B.

<table>
<tr><td colspan="6">All attack cases: 100,000 times. P_E = 0.47</td></tr>
<tr><td colspan="2">Retreat: 11840 times</td><td colspan="4">Continue attack as planned: 88,160 times</td></tr>
<tr><td rowspan="4">Undetected: 1,036 times</td><td rowspan="4">Early detection: 10,804 times</td><td rowspan="4">Undetected: 429 times</td><td colspan="3">Detected: 87,731 times</td></tr>
<tr><td rowspan="3">Uninterrupted: 2,158 times</td><td colspan="3">Interrupted: 85,573 times</td></tr>
<tr><td colspan="2">Not neutralized: 50,410 times</td><td rowspan="2">Neutralized: 35,163 times</td></tr>
<tr><td>Left facility and complete mission before shootout is over: 15,502 times</td><td>Adversaries neutralize responders: 34,908 times</td></tr>
</table>

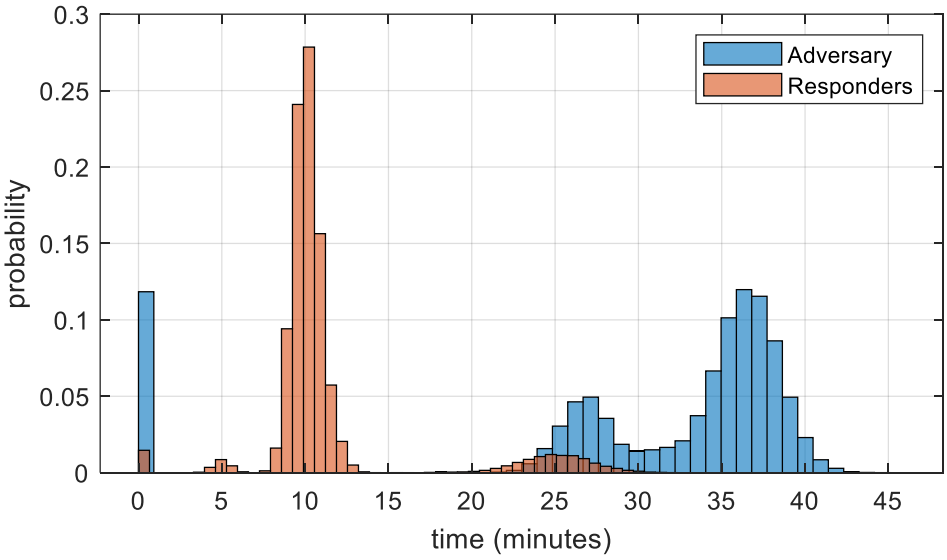


Figure A-7. Timeline histogram for theft target 3 PPS B.

Table A-8. Theft target 3 PPS C.

<table>
<tr><td colspan="7">All attack cases: 100,000 times. P_E = 0.43</td></tr>
<tr><td colspan="2">Retreat: 11,730 times</td><td colspan="5">Continue attack as planned: 88,270 times</td></tr>
<tr><td rowspan="4">Undetected: 999 times</td><td rowspan="4">Early detection: 10,731 times</td><td rowspan="4">Undetected: 443 times</td><td colspan="4">Detected: 87,827 times</td></tr>
<tr><td rowspan="3">Uninterrupted: 8939 times</td><td colspan="3">Interrupted: 78,888 times</td></tr>
<tr><td colspan="2">Not neutralized: 47941 times</td><td rowspan="2">Neutralized: 30,947 times</td></tr>
<tr><td>Left facility and complete mission before shootout is over: 16,700 times</td><td>Adversaries neutralize responders: 31,241 times</td></tr>
</table>

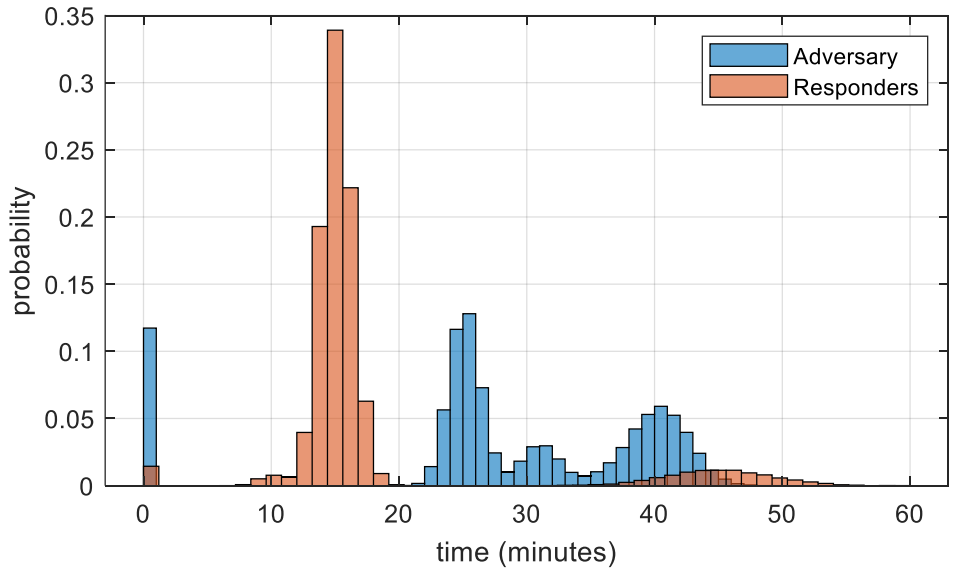


Figure A-8. Timeline histogram for theft target 3 PPS C.

Table A-9. Sabotage target with PPS A.

<table>
<tr><td colspan="6">All attack cases: 100,000 times. P_E = 0.75</td></tr>
<tr><td colspan="2">Retreat: 11,799 times</td><td colspan="4">Continue attack as planned: 88,201 times</td></tr>
<tr><td rowspan="4">Undetected: 1,007 times</td><td rowspan="4">Early detection: 10,792 times</td><td rowspan="4">Undetected: 409 times</td><td colspan="3">Detected: 87,792 times</td></tr>
<tr><td rowspan="3">Uninterrupted: 0 times</td><td colspan="2">Interrupted: 87,792 times</td></tr>
<tr><td colspan="2">Not neutralized: 49,160 times</td><td rowspan="2">Neutralized: 38,632 times</td></tr>
<tr><td>Left facility and complete mission before shootout is over: 10,653 times</td><td>Adversaries neutralize responders: 38,507 times</td></tr>
</table>

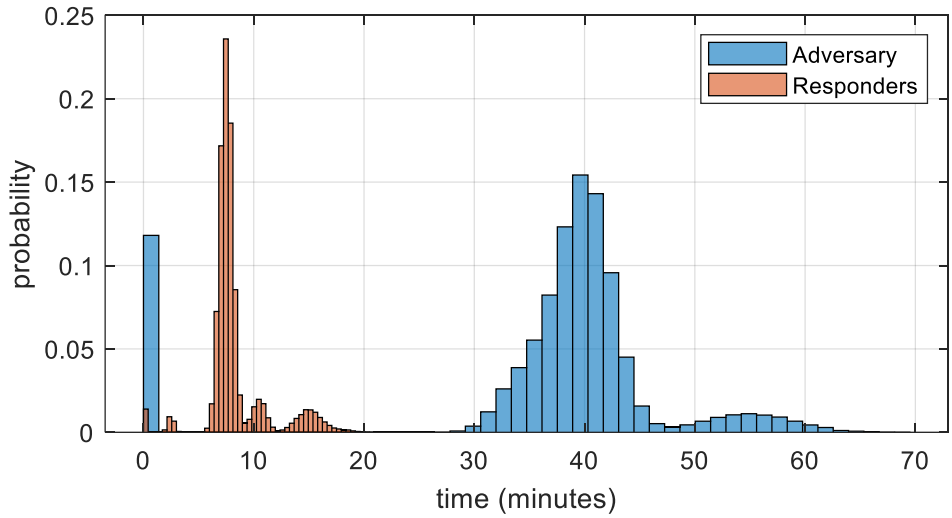


Figure A-9. Timeline histogram for sabotage target with PPS A.

Table A-10. Sabotage target with PPS B.

<table>
<tr><td colspan="6">All attack cases: 100,000 times. P_E = 0.75</td></tr>
<tr><td colspan="2">Retreat: 11,879 times</td><td colspan="4">Continue attack as planned: 88,121 times</td></tr>
<tr><td rowspan="4">Undetected: 998 times</td><td rowspan="4">Early detection: 10,881 times</td><td rowspan="4">Undetected: 425 times</td><td colspan="3">Detected: 87,696 times</td></tr>
<tr><td rowspan="3">Uninterrupted: 16 times</td><td colspan="2">Interrupted: 87,680 times</td></tr>
<tr><td colspan="2">Not neutralized: 49,736 times</td><td rowspan="2">Neutralized: 37,944 times</td></tr>
<tr><td>Left facility and complete mission before shootout is over: 11,410 times</td><td>Adversaries neutralize responders: 38,326 times</td></tr>
</table>

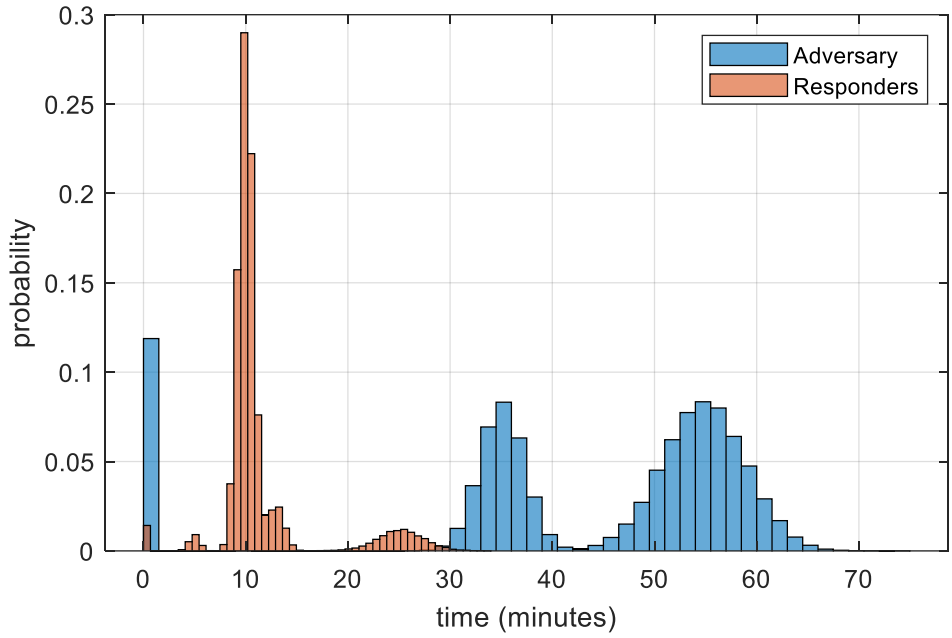


Figure A-10. Timeline histogram for sabotage target with PPS B.

Table A-11. Sabotage target with PPS C.

<table>
<tr><td colspan="6">All attack cases: 100,000 times. P_E = 0.72</td></tr>
<tr><td colspan="2">Retreat: 11,764 times</td><td colspan="4">Continue attack as planned: 88,236 times</td></tr>
<tr><td rowspan="4">Undetected: 953 times</td><td rowspan="4">Early detection: 10,811 times</td><td rowspan="4">Undetected: 410 times</td><td colspan="3">Detected: 87,826 times</td></tr>
<tr><td rowspan="3">Uninterrupted: 8,647 times</td><td colspan="2">Interrupted: 79,179 times</td></tr>
<tr><td colspan="2">Not neutralized: 47,778 times</td><td rowspan="2">Neutralized: 31,401 times</td></tr>
<tr><td>Left facility and complete mission before shootout is over: 16,591 times</td><td>Adversaries neutralize responders: 31,187 times</td></tr>
</table>

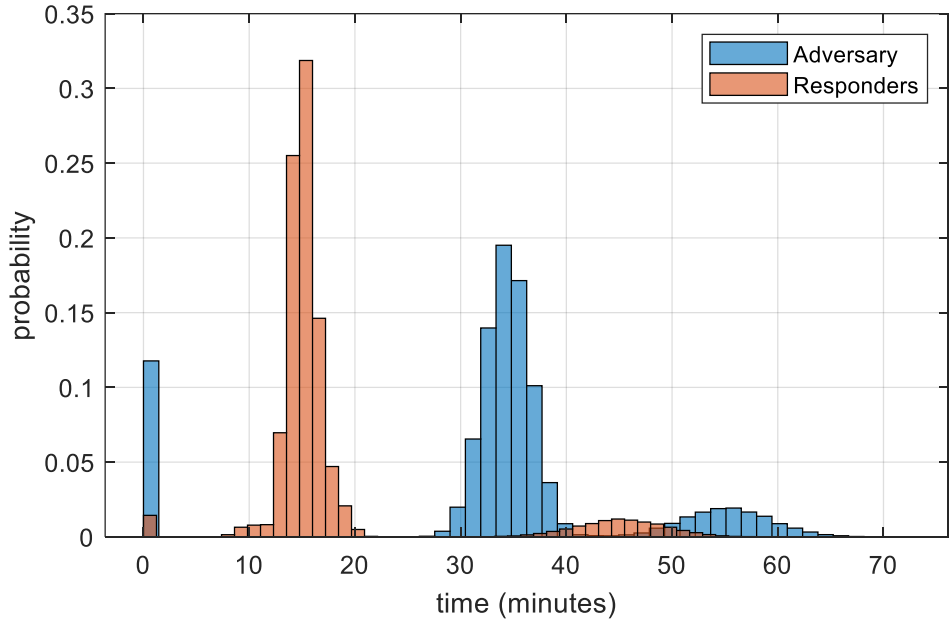


Figure A-11. Timeline histogram for sabotage target with PPS C.