# Development of a Dynamic Event Tree Branching Methodology to Integrate Safety and Physical Security Analyses

Dissertation

Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy in the Graduate School of The Ohio State University

By

Brian Elliott Cohn

Graduate Program in Nuclear Engineering

The Ohio State University

2020

Dissertation Committee

Tunc Aldemir, Advisor

Carol Smidts

Dean Wang

Adam Williams

# Abstract

Physical security for nuclear power plants (NPPs) relies on a method of vital area identification (VAI) to determine locations within the NPP to protect. The VAI methodology uses traditional probabilistic risk analysis (TPRA) methods to identify target sets, locations in the NPP that can result in damage to the reactor core if sabotaged. A vital area set is a combination of locations from each identified target set, such that reactor core damage cannot occur if all vital areas are protected from sabotage. However, challenges remain when evaluating the effectiveness of a NPP's physical protection system (PPS). Metrics for PPSs are based on vital areas; if a vital area is sabotaged, the PPS is judged to have failed. These metrics fail to capture the dynamics of NPP systems at play. Even if one or more vital areas are lost, the reactor core may not be at risk due to additional operational NPP systems or mitigating actions that can be performed by operators to provide additional cooling to the reactor core. Computer models of PPSs and of safety systems at NPPs exist, but these models are not integrated into TPRA.

Dynamic probabilistic risk analysis (DPRA) differs from TPRA in that DPRA methodologies explicitly account for time when modeling a system. One common DPRA method uses dynamic event trees (DETs) to drive computer models of the system under consideration. DETs allow an analyst to systematically explore uncertainties in the timing and ordering of events.

Several DET drivers have been developed to mechanize the DET generation process, usually each linked to a single computer code simulating NPP operation under normal and accident conditions. One of these is the ADAPT DET driver, developed by The Ohio State University for Sandia National Laboratories. While the ADAPT DET driver has recently been upgraded to allow analysts to use multiple simulators for DET generation, the current methodology requires analysts to determine a priori when each simulator will be run. A case study involving the international shipment of spent nuclear fuel is performed to illustrate limitations of the current DET generation methodology.

The goal of this work is twofold: i) develop a methodology that allows analysts to use DETs to resolve some of the challenges caused by single simulator requirement, and, ii) apply the developed methodology to a combined safety and security (2S) analysis. The new methodology allows analysts to run multiple simulators quasi-simultaneously within ADAPT framework without pre-specifying when each individual simulator needs to be run. A second case study is performed to demonstrate the new methodology by splitting a Scribe3D simulation into multiple separate simulations that interact as necessary.

This new methodology is then applied to a case study integrating 2S analyses. Scribe3D is used to construct a security force-on-force model, which tracks the locations of all entities within the NPP as well as what systems are damaged and at what times. A MELCOR model is similarly constructed to track the consequences of losing systems on the reactor core and possible radionuclide releases. The MELCOR model additionally

simulates the effects of mitigation actions by operators and the implementation of FLEX equipment.

The case studies included in this work are not intended to provide a comprehensive investigation of an integrated 2S analysis. Rather, the case studies serve to demonstrate the capabilities of the new methodology and serve as a potential basis for performing 2S analysis in the future. The case studies illustrate how a fuller understanding of the consequences of reactor sabotage can be accomplished using the new methodology, which can be helpful when developing an NPP protection strategy.

The new methodology developed in this dissertation creates a common framework for disparate phenomena that cannot be captured by any one simulator to be jointly evaluated. This framework links multiple simulators together using time to resolve potential conflicts between simulators and is used to integrate the timing and ordering of both sabotage and recovery actions for a NPP. This integrated 2S analysis mechanistically determines the consequences of sabotage to NPP systems based on the timing and ordering of safety and security events.

# Dedication

Dedicated to all those who have fallen in the struggle for a better world.

# Acknowledgments

I would like to thank Professor Tunc Aldemir for his endless patience and guidance during my PhD work. His expertise in nuclear risk analysis has been invaluable to me several times over, and this dissertation could not have been successful without him.

Doug Osborn has generously mentored me through my years at Sandia and this work could not have occurred without his assistance.

No work of merit can be accomplished by one person and this dissertation is no exception. Discussions with Zac Jankovsky inspired the methodological framework used in this work. Todd Noel provided modifications to the Scribe3D code to enable its use with the LS/TS method. I am furthermore grateful to those researchers at Sandia, too many to name, whom I have collaborated with for model and scenario development. What I have learned about nuclear security through this dissertation pales in comparison to what they have taught me.

Finally, I am eternally grateful to my family for standing with me every step of the way. None of this could have happened without their support.

# Vita

2010 . . . . . B.S. Physics,
Arizona State University

2018 . . . . . M.S. Nuclear Engineering,
The Ohio State University.

2016-present . . . . . .Graduate R&D Intern,
Sandia National Laboratories.

Publications

1. B. Cohn, A. Alfonsi, D. Mandelli, and C. Rabiti, “Comparison of Surrogate Models with Physical Models for Dynamic Probabilistic Risk Analysis Using the RAVEN Code,” in *Transactions of the American Nuclear Society*, Las Vegas, NV, 2016.

2. A. Williams, D. Osborn, K. Jones, E. Kalinina, B. Cohn, M. J. Parks, E. Parks, E. Johnson, and A. Mohagheghi, “A New Look at Transportation Security: A Complex Risk Mitigation Framework for the Security of International Spent Nuclear Fuel Transportation,” in *The International Conference on Nuclear Security: Commitments and Actions*, Vienna, Austria, 2016.

3. B. Cohn, R. Denning, T. Aldemir, J. Hur, and H. Sezen, “Implementation of Surrogate Models within RAVEN to Support SPRA Uncertainty Quantification,” in *Proceedings of the 27$^{th}$ European Safety and Reliability Conference (ESREL 2017)*, Portorož, Slovenia, 2017.

4. B. Cohn, R. Denning, T. Aldemir, J. Hur, and H. Sezen, “Surrogate Model Selection in RAVEN for Seismic Dynamic PRA/PSA,” in *International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA 2017)*, Pittsburgh, PA, 2017.

5. A. Williams, D. Osborn, K. Jones, E. Kalinina, B. Cohn, A. Mohagheghi, M. DeMenno, M. Thomas, M. J. Parks, E. Parks and B. Jeantete, "System Theoretic Frameworks for Mitigating Risk Complexity in the Nuclear Fuel Cycle," Sandia National Laboratories, Albuquerque, 2017.

6. B. Cohn, J. Hur, R. Denning, T. Aldemir, and H. Sezen, “Convergence of Varied Surrogate Models for Seismic Dynamic PRA/PSA,” in *Probabilistic Safety Assessment and Management 14*, Los Angeles, CA, 2018.

7. A. Williams, D. Osborn, J. Bland, J. Cardoni, B. Cohn, C. Faucett, L. Gilbert, R. Haddal, S. Horowitz, M. Majedi, and M. Snell, “System Studies for Global Nuclear Assurance & Security: 3S Risk Analysis for Small Modular Reactors (Volume I) Technical Evaluation of Safety Safeguards & Security,” Sandia National Laboratories, Albuquerque, 2018.

8. B. Cohn, A. Williams, and T. Aldemir, “Exploring Integrated Safety/Security Dynamic Probabilistic Risk Assessments (DPRA) for Nuclear Power Plants,” in *International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA 2019)*, Charlotte, SC, 2019.

9. D. Osborn, M. J. Parks, R. Knudsen, K. Ross, C. Faucett, T. Haskin, P. Kitsos, T. Noel and B. Cohn, “Modeling for Existing Nuclear Power Plant Security Regime,” Sandia National Laboratories, Albuquerque, 2019.

10. A. Williams, B. Cohn, and D. Osborn, “Security, Safety, and Safeguards (3S) Risk Analysis for Small Modular Reactors” in *Proceedings of the Institute of Nuclear Materials Management*, Palm Desert, CA, 2019.

11. A. Williams, D. Osborn, and B. Cohn, “Advancement of Dynamic Assessment Methodologies for Transportation Security,” in *19$^{th}$ International Symposium on the Packaging and Transportation of Radioactive Materials (PATRAM 2019)*, New Orleans, LA, 2019.

12. B. Cohn, “Using Reactor Simulations to Improve Security Analysis,” presented in *The 2020 Power Plant Simulation Conference*, Chattanooga, TN, 2020.

13. B. Cohn, T. Noel, T. Haskin, D. Osborn, and T. Aldemir, “Quasi-Simultaneous System Modeling in ADAPT,” in *Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference*, Venice, Italy, 2020.

## Fields of Study

Major Field: Nuclear Engineering

# Table of Contents

# List of Tables

# List of Figures

# List of Acronyms

**2S** Safety-Security

**AFW** Auxiliary Feedwater

**ALM** Adversary Logic Model

**ASD** Adversary Sequence Diagram

**ATR** Advanced Thermal Reactor

**AVERT** Automated Vulnerability Evaluation for Risks of Terrorism

**BC** Branching Condition

**BE** Basic Event

**BN** Branch Number

**BTRA** Bioterrorism Risk Assessment

**BWR** Boiling Water Reactor

**CANDU** Canadian Pressurized Heavy Water Reactor

**CAS** Central Alarm Station

**CDP** Critical Detection Point

**CPPNM** Convention on the Physical Protection of Nuclear Material

**CR** Control Room

**CST** Condensate Storage Tank

**CV** Control Volume

**CsI** Cesium Iodide

**DBA** Design Basis Accident

**DBT** Design Basis Threat

**DEPO** Design and Evaluation Process Outline

**DET** Dynamic Event Tree

**DOE** Department of Energy

**DPRA** Dynamic Probabilistic Risk Assessment

**EDG** Emergency Diesel Generator

**ET** Event Tree

**FT** Fault Tree

**FoF** Force-on-Force

**GUI** Graphical User Interface

**IAEA** International Atomic Energy Agency

**IEMO** Initiating Event of Malicious Origin

**ITC** International Training Course

**JCATS** Joint Conflict And Tactical Simulation

**LLE** Local Law Enforcement

**LLNL** Lawrence Livermore National Laboratory

**LOLA** Loss of Large Area Analysis

**LOOP** Loss of Outside Power

**LPNPP** Lone Pine Nuclear Power Plant

**LS** Leading Simulator

**LS/TS** Leading Simulator/Trailing Simulator

**MAAP** Modular Accident Analysis Program

**NAR** Nuisance Alarm Rate

**NPP** Nuclear Power Plant

**NRC** United States Nuclear Regulatory Commission

**NSS** Nuclear Security Series

$\boldsymbol{P_E}$ Probability of Effectiveness

$\boldsymbol{P_I}$ Probability of Interruption

**PIDAS** Perimeter Intrusion Detection and Assessment System

$\boldsymbol{P_N}$ Probability of Neutralization

**PPS** Physical Protection System

**PWR** Pressurized Water Reactor

**RAMCAP** Risk Analysis and Management for Critical Asset Protection

**RIMES** Risk Informed Management of Enterprise Security

**RWST** Refueling Water Storage Tank

**SAS** Secondary Alarm Station

**SME** Subject Matter Expert

**SNF** Spent Nuclear Fuel

**SNL** Sandia National Laboratories

**SSC** System, Structure, and Component

**TE** Top Event

**TMI** Three Mile Island

**TPRA** Traditional Probabilistic Risk Analysis

**TS** Trailing Simulator

**UHS** Ultimate Heat Sink

**VA** Vulnerability Assessment

**VAI** Vital Area Identification

**VESPA** Vulnerability Evaluation Simulating Plausible Attacks

**VVER** Russian Pressurized Light Water Reactor

**WA** Worlds Abstraction

# Chapter 1 - Introduction

This chapter presents the research problem addressed by the dissertation. Section 1.1 gives a brief description of challenges using dynamic methodologies with nuclear security. Section 1.2 describes the goals of this research and its anticipated effects on the state of the art. Section 1.3 describes the scope of work performed in this effort and Section 1.4 describes the organizational structure of chapters in the dissertation.

## 1.1 Problem Description

Nuclear power plants (NPPs) feature a large number of systems, structures, and components (SSC). These SSCs interact in complex and dynamic ways, such that the overall performance of an NPP cannot be understood from the behavior any one SSC. In addition, the NPP systems can be highly interconnected, such that viewing each system in isolation will not present the complete picture. An example is the situation when considering emergency response systems and security systems for NPPs. To maximize the emergency response system's capability, it is desirable to allow emergency responders to arrive at the NPP as rapidly as possible. To maximize the security system's capability, it is necessary to perform thorough searches and checks on all vehicles and personnel arriving at an NPP for any reason. This process can be slow and would delay emergency response personnel.

A NPP's physical protection system (PPS) is a subsystem of the NPP's overall security systems. PPS are used to protect a NPP from adversary attacks (see Appendix A for a more detailed description of PPS). The PPS does this by identifying vital areas, locations within the NPP that need to be protected from sabotage. While security analysis is designed to ensure that vital areas are protected from sabotage, security analysis is unable to determine the consequences of successful sabotage of some vital areas. Determining the consequences of losing NPP equipment is the domain of safety analysis. Security analysis assumes that the loss of any vital area necessarily results in a release of radionuclides to the public [1]. Current approaches to account for the interaction between safety and security analysis, as well as their limitations, are overviewed in Section 4.3 of this dissertation. Several of the identified limitations of the current approaches used to account for interactions between nuclear safety and nuclear security analysis are due to the static nature of these approaches. These approaches are unable to consider decision-making by adversaries or the differences in the timing of security events vs. safety events.

Dynamic probabilistic risk analysis (DPRA) [2] as applied to engineered systems is a risk analysis method that considers the interaction among hardware/process/software/human behavior in addition to the likelihood of events and their consequences. DPRA uses computer simulations to capture the impacts of phenomena on systems. As no computer simulation has been created which simultaneously models the security system and the safety systems and their interaction, however, DPRA would need to use separate models for the security system and the plant response though the safety system. A challenge with this approach is that the DPRA

methodology would need to transfer data between the security model and the safety model. Additionally, as both security models and safety models are typically explicit-time models, the DPRA methodology needs to run both models simultaneously. Nuclear safety computer models such as MELCOR [3] and RELAP [4] are designed to operate as stand-alone computer models. These codes are not designed to accept input from external sources while running or to limit the speed that the model runs at to maintain pace with another running model. The DPRA methodology therefore needs to have the capability to emulate such functionality.

## 1.2 Objectives

The objective of this work is to create a general methodology using the dynamic event tree (DET) approach (see Section 4.2) of DPRA to overcome the current limitations of joint safety-security analyses. The proposed methodology enhances the state of the art by providing a general coupling scheme of multiple explicit-time safety and security simulators into a single analysis. The methodology aims to:

- enable DETs to integrate multiple explicit-time system codes, passing information back and forth as needed;
- relieve the analyst from needing to determine which simulator is called on at each DET branch (see Section 4.2);
- provide the ability to use a risk-informed approach in determining the vital areas in security analysis;
- provide tools to incorporate recovery and mitigation actions post-sabotage into security analyses, and;

- incorporate the system safety effects of losing NPP equipment into security analysis for NPPs, including the magnitude of a possible radionuclide release.

The emerging process from the proposed approach will result in developing more realistic protection strategies for NPPs, and allow for equipment to be prioritized from a security point of view based on a more finely-graded approach than is done currently.

## 1.3 Scope

This work develops a methodology to run multiple simulators in a quasi-simultaneous fashion to integrate safety and physical security analyses using the DET approach. Elements of cyber security are not considered in this work. This objective is accomplished by the introduction of an advanced branching process (Section 6.2). The current state of the art for DETs [5] allows an analyst to use multiple simulators in one DET, with a choice of simulator to use for each branch. Instead of each branch running a single simulator, as the state of the art method allows, each branch in this work uses multiple concurrent models to obtain the full system behavior.

These capabilities of the proposed approach are demonstrated through three case studies. Case Study 1 uses the current state-of-the-art DET behavior to perform a joint safety-security (2S) analysis (Section 6.1). This case study demonstrates the limitations of current DET capabilities when using multiple simulators in one analysis. Case Study 2 demonstrates the effectiveness of the newly-developed methodology to replicate the behavior from a single simulator (Section 6.3). Case Study 3 uses the proposed methodology on a combined 2S system to explore the safety effects of an adversary attack on a NPP (Chapter 7). Case 3 also accounts for coping times, determining how

long after sabotage actions the NPP operators would have to prevent core damage, and characterizing the release of radionuclides based on adversary and security personnel actions.

## 1.4 Dissertation Overview

The dissertation is divided into a total of eight chapters, including this introductory chapter. Chapters 2 through 5 describe different background elements for the problem under consideration. Chapter 2 provides an overview of nuclear security regulations, including the historical context these regulations were developed under, and highlights some of the potential challenges that exist under the current regulatory structure.

Chapter 3 provides an overview of the principles of nuclear security using the framework of the Design and Evaluation Process Outline (DEPO) methodology [6]. Chapter 3 additionally includes an introduction to current methodologies used to determine the effectiveness of a PPS.

Chapter 4 introduces the principles of risk analysis as used by nuclear safety analysts. These principles include an overview of the fault tree (FT) and event tree (ET) methodology used in traditional probabilistic risk analysis (TPRA), and how DETs are used to address some phenomena that TPRA has challenges in modeling. Chapter 4 also provides a history of past attempts to incorporate nuclear safety and security analyses and some of the challenges that were discovered through these efforts.

Chapter 5 provides an overview of selected computerized analysis codes that have been developed to either model security or safety phenomena at NPPs. These codes

include the tools used within this dissertation and many of the commonly-used alternative codes. Chapter 5 additionally introduces some DPRA tools and explains the differences between these tools.

Chapter 6 introduces the overall methodology. Case Study 1 uses the current state of the art in integrating nuclear safety and nuclear security disciplines and illustrates some of the practical limitations. Case Study 2 then uses the proposed methodology to demonstrate the feasibility of the approach on a simple system. The proposed approach using a scenario divided between two models is compared to the same scenario analyzed as a single model to determine if the proposed methodology can accurately transfer information between models.

Chapter 7 presents Case Study 3 that demonstrates an integrated 2S analysis of a scenario. In this scenario, adversaries are effective in sabotaging a vital area. The consequences of the sabotage, including degradation, are modeled. In addition, mitigation and repair actions that are attempted and the effects of these actions are incorporated into the plant evolution.

Chapter 8 concludes the dissertation with a summary of contributions made by the current research and highlights identified avenues for future work. These contributions include allowing for the integration of safety and security phenomena, as well as providing the capability to consider system dynamics when generating target sets, i.e., locations in the NPP that can result in damage to the reactor core if sabotaged.

# Chapter 2 - Nuclear Security Regulatory Structure

Nuclear security regulations are constructed to ensure that NPPs can maintain secure operation and produce electricity. This chapter provides a discussion of the history and current practice of nuclear security regulation. Section 2.1 covers the background on domestic nuclear security regulation pre-9/11, while Section 2.2 describes how these regulations evolved after 9/11. Section 2.3 describes international regulations and best practice, and Section 2.4 presents some challenges in the current regulatory structure.

## 2.1 Background of Domestic Nuclear Power Plant Security

The goal of any commercial NPP is to maintain safe and secure continuous operation in order to produce electricity. Nuclear safety is concerned with the protection of the public from failures of safety systems or inadvertently erroneous operation of NPPs. Nuclear security is concerned with the protection of the public from malicious acts, either through sabotage of NPP systems or diversion of nuclear material for illicit purposes. Nuclear security, however, has generally lagged behind nuclear safety as a discipline, and made use of nuclear safety insights. This lag dates back to the Atomic Energy Act of 1954 [7] which directed the Atomic Energy Commission to grant licenses to applicants “who are equipped to observe and who agree to observe such safety standards to protect health and to minimize danger to life or property as the Commission

may by rule establish". Nuclear security, therefore, has often relied on nuclear safety practices, particularly when it comes to analysis methods.

Until the late 1970s, safety of NPPs was not generally considered to be within the domain of risk assessment but was instead based on the deterministic design and operational rules (e.g. safety systems must supply enough cooling to protect against the largest credible LOCA, or operations must ensure core power does not exceed proscribed limits [8]). These limits were based on expert judgment and used conservative assumptions to ensure that the plant would remain safe even in the most severe credible scenarios. The deterministic mindset for safety essentially resulted in NPP security that was commensurate to typical industrial levels of security.

In 1975 the United States Nuclear Regulatory Commission (NRC) published the Reactor Safety Study; WASH-1400 [9]. This study used a novel analysis method known as TPRA to generate ETs and FTs that could identify combinations of component failures which result in an eventual reactor core meltdown and release of radionuclides to the environment. Components were assigned failure probabilities, which when combined with Boolean algebra could determine the probabilities of failure of systems and of an entire NPP.

The adoption of TPRA moved safety from a deterministic approach and into the domain of risk. Through TPRA, NPPs and the NRC were able to determine the effects of different accident sequences on the system wide risk, including accidents, such as the one that occurred at Three Mile Island (TMI) [10], which were believed to be less severe than the design basis accidents (DBAs) used for regulation. Frequently, PRA studies

concluded that such less severe events may still have a substantial effect on risk associated with NPP operation. As a result, the NRC began adopting risk-informed regulations, which are regulations that do not depend specifically on the calculated risk of NPP operation but used as one factor by the NRC for rulemaking.

However, nuclear security has not yet made use of risk-informed regulations, and instead continues to use prescriptive regulations. In 1977, the NRC implemented rule 10 CFR 73.55 [11] and proposed changes to rule 10 CFR 73.20 [12], both with regards to the physical protection of nuclear reactors, often described as safeguards by the NRC[1]. These rules called for performance requirements ensuring that NPP operators would be able to protect against industrial sabotage through both force and stealth, perpetrated by either outsiders or insiders, and potentially both working in collaboration. The rules additionally required that each area containing vital equipment to be designated and protected as a vital area located within a protected area, as well as mandating several practices and procedures, such as minimum and nominal numbers of guards.

In part due to these regulatory changes, the United States Department of Energy (DOE) undertook research to identify vital areas at NPPs in a systematic fashion. For example, Sandia National Laboratories (SNL) developed a NPP vital area identification (VAI) process based on FT analysis. The approach considers adversary actions which can lead to direct radiological sabotage [13]. In this approach, top-level events such as the release of radioactive material from a NPP are logically conditioned on lower-level

[1] The term 'safeguards' is used throughout the rest of this dissertation to refer to the program of international safeguards supporting the Treaty on the Non-Proliferation of Nuclear Weapons.

events with Boolean operators. A provided example in [13] is that the release of radioactive material occurs if:

1. material is released from the reactor core to containment OR,
2. from spent fuel containment OR,
3. from the radwaste system to containment.

These events are similarly decomposed until the analyst is left with basic events originating from individual component failures within the system. The locations containing these individual components are designated as vital areas in accordance with regulations.

In the 1980s, in the wake of the TMI accident, which boosted the credibility of the ET/FT analysis pioneered by WASH-1400, NPP operators began constructing TPRAs of their own plants [14] to identify accident sequences which constituted the main contributors to risk. During this analysis, NPPs created FTs of their entire plant, identifying which combinations of component failures listed as basic events. NPP operators then used these FTs to determine combinations of safety systems that, if protected, would be sufficient to maintain the reactor core and designated this equipment as the extent of vital equipment and their locations as vital areas in need of protection [15, 16]. Additionally, NPPs used these vital area sets to create adversary target sets as the Boolean complement of the vital area sets. The approach considers anticipated adversary capabilities which can lead to direct and indirect radiological sabotage.

Despite widespread adoption of VAI and target set analysis by NPPs throughout the 1980s, the NRC did not formally consider mandating NPPs to construct target sets

until 1999. In 1999, the NRC's Safeguards Performance Assessment Task Force [17] recommended to the NRC commissioners that "The regulations be modified to require power reactor licensees to identify target sets, develop protective strategies, and exercise these strategies on a periodic basis," while the NRC staff, "develop[ed] a regulatory guide to outline the process for developing target sets and sabotage scenarios, as well as to detail acceptable means of conducting the exercises." However, before these recommendations could be put into force, the terrorist attacks of September 11, 2001 (9/11 event) occurred and drastically altered NRC priorities regarding nuclear security.

## 2.2 Domestic Nuclear Power Plant Security Regulations Post-9/11 Event

After the 9/11 event, a new focus was given to nuclear security. In early 2002 [18], the NRC issued an order requiring additional security measures be taken at NPPs, including loss of large area analysis (LOLA), which falls into the realm between safety analysis and security analysis. LOLA [19] was conceived due to the potential effects that a large commercial aircraft could have on a NPP site if it were to crash into plant structures, but the analysis was general enough to include effects from other explosions or fires, which can arise due to accident rather than malice. The thrust of LOLA is to ensure that means of cooling and maintaining the reactor are such that the complete loss of several adjacent rooms within a NPP facility would not lead to core damage or an unacceptable release of radionuclides to the environment.

Many of the insights of LOLA [19] (i.e., the need to avoid co-locating safety equipment and to construct barriers between separate trains of equipment) inform VAI which the NRC issued guidance on performing in 2008. At the forefront of these insights

is the need to construct substantial physical barriers with restricted access. While the need for physical protection (such as barriers around critical equipment) was understood, LOLA added the consideration of adding physical barriers separating safety system trains to protect one train from an event that causes the loss of another train. Additionally, LOLA acknowledged the negative effects maintaining this separation could have during an emergency, where unrestricted access by emergency personnel to safety equipment would be otherwise desirable.

The 2008 NRC guidance [20] on VAI ties the creation of vital areas and target sets to the ET/FT methodology of Level 1 PRAs, in a similar manner as the 1975 WASH-1400 study [9]. This 2008 NRC guidance calls for the following steps:

1. Determine inventories of nuclear material with sabotage concern;
2. Evaluate direct dispersal as a potential risk;
3. Identify initiating events which can lead to radiological release and systems required for mitigation of events;
4. Construct adversary logic model (ALM) to determine combinations of events which could lead to core damage;
5. Eliminate events from the ALM that the design basis threat adversaries are unable to perform;
6. Identify locations within the NPP that the events remaining in the ALM can be performed and replace the events in the sabotage logic model with their corresponding areas;

7. Solve the ALM to identify minimum target sets of areas that could lead to successful radiological sabotage;

8. Find the Boolean complement of the target areas to produce candidate vital area sets, areas within the NPP that if all protected will prevent radiological sabotage, and;

9. Select the vital area set that is most advantageous to protect.

The vital areas constructed through these steps serve as the foundation of security activities for NPPs [21].

## 2.3 International Nuclear Security Guidance

In the international sphere, there are few enforceable regulations concerning nuclear security; rather they are guidance and recommendations. The only widely adopted international nuclear security regulations considered to have legal force are in the Convention on the Physical Protection of Nuclear Materials (CPPNM) [22]. The CPPNM binds States to ensure a level of protection of nuclear facilities and materials in transit. The CPPNM states that States must provide a “graded approach” to nuclear security to prevent theft and preclude or mitigate radiological sabotage. Nuclear material in the CPPNM is placed into one of three adversary attractiveness categories and requires increasing levels of protection for that material as the categories increase. According to the CPPNM, these categories of material require physical protection as shown in Table 2-1. In this table, Category I is the highest level of attractiveness and includes all protection measures required for Categories II and III. Category II additionally requires those protection measures established for Category III materials.

Table 2-1 Levels of Physical Protection Required by the CPPNM [22]

| Attractiveness Category | Protection Measures |
|---|---|
| Category III and above | • An area to which access is controlled |
| Category II and above | • Constant surveillance<br>• A physical barrier with a limited number of points of entry |
| Category I | • Access is restricted to persons whose trustworthiness has been determined<br>• Guards are in close communication with appropriate response forces |

Beyond the CPPNM, the International Atomic Energy Agency (IAEA) has published security guidance and best practices for providing physical security as the Nuclear Security Series (NSS). The NSS documents are divided into four sets, depending on the intent of the document. These sets are:

- Nuclear Security Fundamentals
- Nuclear Security Recommendations
- Nuclear Security Implementing Guides
- Nuclear Security Technical Guidance

The NSS Fundamentals outline the basic objectives of a State's physical security regime and necessary elements to include. The NSS Recommendations documents describe ways to organize a State's security regime. The NSS Implementing Guides and Technical Guidance provide increasing levels of detail on how to carry out the NSS Recommendations.

In the NSS Fundamentals [23], the objective of nuclear security is defined as "protect[ing] persons, property, society, and the environment from harmful consequences

of a *nuclear security event*." The document additionally calls for using a risk-informed approach that considers:

> "Potential harmful consequences from criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, associated activities, sensitive information or sensitive information assets, and other acts determined by the State to have an adverse impact on nuclear security".

Included in the IAEA's *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities* [24] are a related set of objectives created for the more specific task of providing physical protection and are also reflected in the CPPNM. These objectives are defined by the IAEA as:

- **To protect against *unauthorized removal*.** Protecting against theft and other unlawful taking of nuclear material
- **To locate and recover missing *nuclear material*.** Ensuring the implementation of rapid and comprehensive measures to locate and, where appropriate, recover missing or stolen *nuclear material*.
- **To protect against *sabotage*.** Protecting *nuclear material* and *nuclear facilities* against *sabotage.*
- **To mitigate or minimize effects of *sabotage*.** Mitigating or minimizing the radiological consequences of *sabotage*.

Notably included in the IAEA's objectives are analysis and mitigation of consequences in the event of a nuclear security event.

## 2.4 Challenges with the Current Nuclear Security Structure

In the current version of 10 CFR 73.55 [25], the NRC requires NPPs to establish a "physical protection program [that] protect[s] against the design basis threat of radiological sabotage" which is later described as "prevent[ing] significant core damage and spent fuel sabotage." Notably with regard to the IAEA physical security objectives, while the NRC regulations require NPPs to protect against unauthorized removal and sabotage, the regulations do not describe recovering missing nuclear material or mitigating the effects of sabotage.

The NRC regulations require the prevention of significant core damage rather than basing physical protection requirements on public health effects or radionuclide releases. Therefore, safety systems such as containment structures that exist to mitigate the effects of core damage on the environment are not considered under NRC regulations. NPPs currently perform Level 2 PRA, which analyzes the evolution of safety accidents from core damage to environmental radionuclide release (e.g., failure or bypass of containment) which are not incorporated into current nuclear security risk assessments.

Additionally, the NRC's guidance on VAI [20] is intended to ensure that one safety train is protected as "vital" to maintain adequate core cooling. However, when performing a vulnerability assessment (VA), the success of the physical protection strategy requires that ***NO*** vital area be sabotaged. A VA assumes that the loss of a vital area causes core damage, as informed by Level 1 PRA. This assumption does not follow, as the VAI methodology is incapable of determining the effects of losing vital areas. VAI establishes that if all vital areas are protected, the plant is protected from core damage,

and an attendant release of radionuclides following core damage. However, if a vital area is lost, the security of the plant is unknown. The NPP may not undergo core damage. The NPP may undergo core damage that does not result in a radiological release. The NPP may undergo core damage and a release of radionuclides.

If a vital area contains equipment for only one safety train, then sabotage of that single vital area would only lead to the loss of one train. However, for safety reasons NPPs can provide cooling to the plant despite the loss of a single safety train. As such, successful radiological sabotage of the NPP core may require sabotaging additional systems beyond one vital area to cause significant core damage, but this is not reflected within current NRC regulation and guidance.

More generally, the VAI process in physical security has some limitations in practice. The FT/ETs that NPPs have developed for safety analysis have assumptions built into them that do not necessarily apply to security events. For example, one assumption that is made for seismic FT/ETs is that all structures which are not built to Category 1 seismic standards are lost. In the physical security setting, however, no systems are lost unless damaged by adversary action. Therefore, vital areas constructed from seismic FT/ETs may not account for the true level of redundant systems in the NPP.

Additionally, TPRA includes all plant states and is largely driven by the full power operation state, which is generally the worst-case scenario. While the same assumptions hold for security analysis, there is some time between the onset of an attack and successful sabotage. This delay shifts the decay power curve and has the possibility of changing which equipment is vital as a function of time. If adversaries are detected

early enough in their mission, shutting down the NPP could lead to equipment that would be vital at full power no longer being vital in the time that it would take adversaries to arrive at and sabotage that equipment. As an example, if the accumulators were normally considered vital equipment, but were predicted to discharge their coolant before adversaries could sabotage the tanks, then it would not be necessary to have the physical protection strategy prevent adversary sabotage rather than delaying it.

Requiring the physical protection strategy to protect equipment that is not necessary for the protection of the NPP has several possible disadvantages. The most immediate of these is economic. Any physical protection strategy requires a number of systems and personnel to maintain, and the costs associated with physical protection rises as more vital areas need to be simultaneously protected.

Beyond the direct costs of protection, expanding a physical protection strategy unnecessarily may increase overall system risk. Part of any risk mitigation strategy, including safety and physical protection, is prioritizing among different risks. For example, if a physical protection strategy requires protecting systems and equipment that a more complete analysis would determine is unnecessary, such a strategy would require taking security resources away from more critical locations or using less-successful protection strategies. As another example, a protection strategy may require that Door X is locked and guarded in order to protect Vital Area Y, even though this configuration increases the difficulty of protecting other vital areas. If a more detailed analysis determines that the loss of Vital Area Y does not result in reactor core damage, then the protection strategy can unlock Door X and reassign its guard to another location,

increasing the protection of the NPP as a whole. It is possible that knowledgeable adversaries will be able to exploit this behavior (e.g., by launching decoy attacks at non-critical systems and drawing protection away from truly critical systems or components for the given plant condition).

This dissertation introduces a DPRA methodology for 2S analysis. The use of DPRA is expected to link the sabotage of NPP equipment to the release of radionuclides, which would allow the NRC to consider consequences to the public to be more directly considered by NRC regulations. In addition, the proposed DPRA methodology would allow the NRC to consider the effects of mitigation systems currently used in safety analysis for security analysis. Creating an integrated 2S methodology through DPRA also allows timing effects of sabotage to be considered explicitly, as well as the immediate plant state during an adversary attack. Finally, considering these additional effects allows NPPs to more precisely determine vital areas and construct more narrowly-tailored protection strategies.

# Chapter 3 - Nuclear Security Analysis

To protect NPPs from malicious action, operators design and construct a PPS. The system has the purpose of preventing adversaries from conducting theft or sabotage on the protected facility. A PPS uses security features, which can range from locked doors to armed responders manning hardened fighting positions. Indeed, NPPs typically use a graded approach to security where more critical are given increased levels of protection than less critical areas in the plant. For the purpose of this dissertation, nuclear security refers solely to physical security. Cyber security, although it uses many of the same principles as physical security, is outside the scope of this work.

In a PPS, the site is divided into several areas, as defined by the NRC in 10 CFR 73.55 [25]. An illustration showing the arrangement of these areas is given in Figure 3-1. The largest of these is the *owner-controlled area*, which is the all the property owned by the site. Located within the owner-controlled area is the *limited access area*. The limited access area is a designated area containing the NPP and nuclear material areas (e.g., dry cask storage) to which access is limited and controlled for physical protection purposes. Within the limited area are *protected areas*. The protected area boundary is delineated by physical barriers and access control to allow only authorized persons to enter the protected area. Within the protected area are one or more *vital areas*. These are the most

secure areas of the plant where adversaries may be able to affect sabotage (direct or indirect) or theft of nuclear materials.

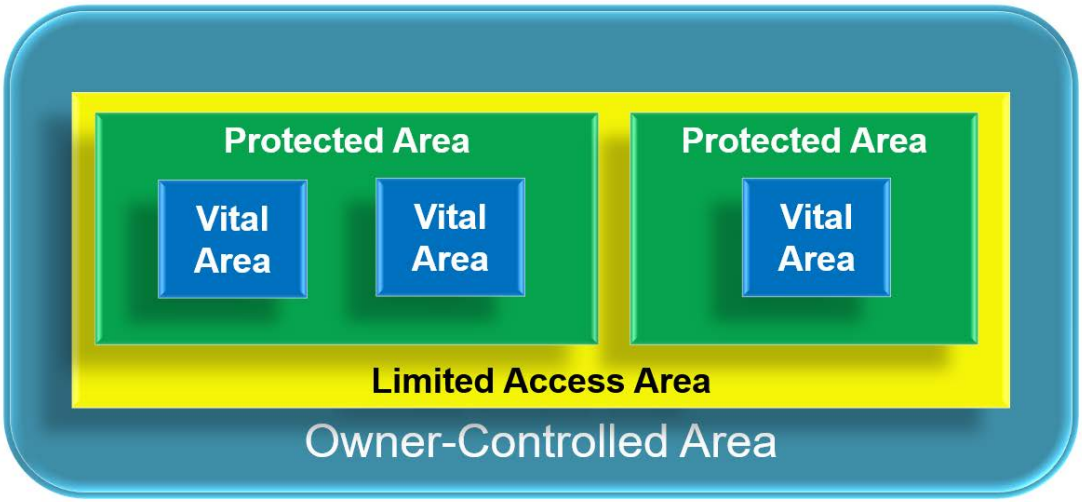


Figure 3-1 Illustration of protection areas at nuclear facilities

There are multiple methods to use for creating a PPS. One method can be to have prescriptive required features in a PPS design. This method is simple to implement, as the required features need only be built as specified [26]. For example, regulations could require a locked door of some construction with a camera monitoring the outside and the NPP could build that specified design. While this approach has the advantage of being simple to implement, the results are not performance-based, and the ability of a PPS designed in this manner against an adversary attack is not ascertained. Several different PPS designs, which all contain exactly the required features, can have wildly different effectiveness against adversaries and this method is unable to distinguish between these different PPS designs. For example, a PPS that requires a locked door and a camera can have different levels of effectiveness if the camera has a view of the door or of the hallway leading up to the door. Furthermore, a camera that has its view blocked by

furniture meets the requirements but is not effective. Finally, as the prescriptive measures exist independent of an adversary, a PPS constructed to meet feature requirements is static when the capabilities of adversaries change. A PPS built in this way can update only when the list of required features changes.

Another method of designing a PPS is to use expert elicitation by an expert with experience designing PPSs [26]. Depending on the experts selected, there may be a large degree of understanding for security system installations that are more or less effective, and expert elicitation is less expensive than many other design methods. However, this method also has the disadvantage of not being performance-based. In addition, the design of the PPS may vary substantially depending on the experts used in the construction, due to personal preferences and biases among different experts for various security technologies.

In the United States, DEPO is an approach which is designed for use by NPPs, and used by the NRC for evaluation [6]. The DEPO methodology was first developed by SNL in the 1970s [27] as an adaptation of previous research on a systems level approach to protecting critical nuclear assets. This is a performance-based methodology that outputs justifiable and measurable system performance metrics against a specified threat. Figure 3-2 shows the process flow of the DEPO methodology.

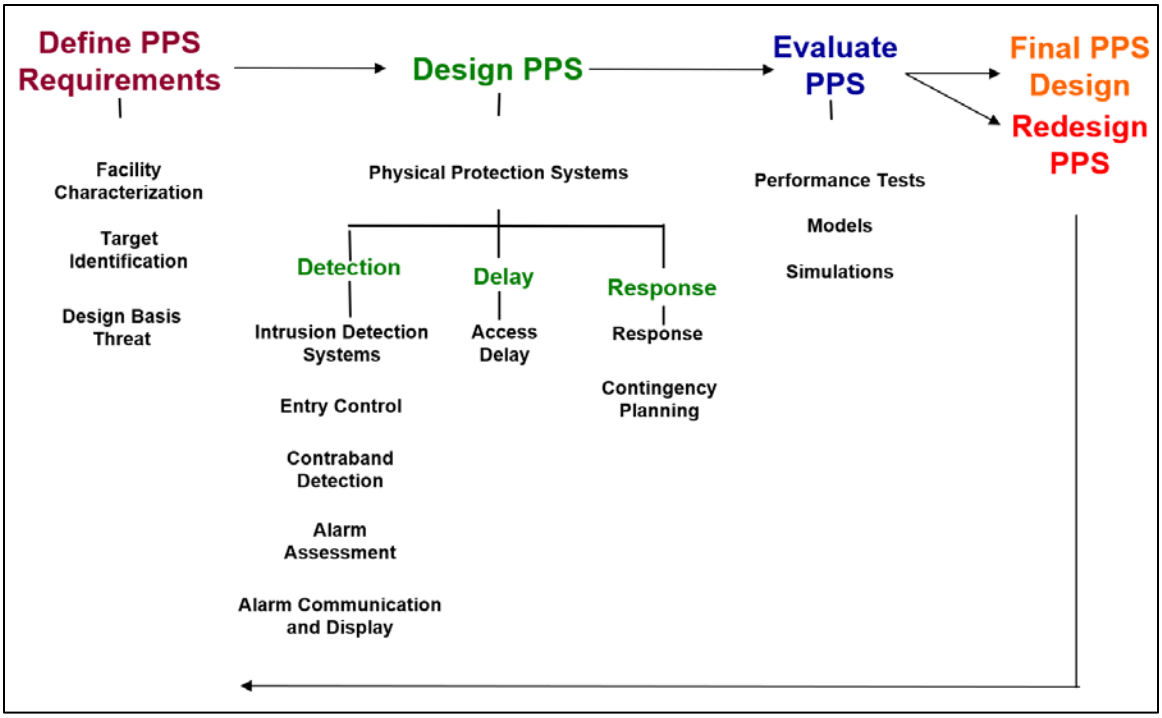


Figure 3-2 Design Evaluation Process Outline flowchart [6]

The DEPO methodology first requires the facility to understand the capabilities of adversaries and locations within the facility that an adversary can accomplish their goals. The foundation of the built PPS, as envisioned by the DEPO process, is to perform the three pillars of detection, delay and response to adversaries. Detection is necessary to initiate the physical protection process. After an adversary has been detected, delay serves to prevent the adversaries from reaching their target until response can interrupt the adversaries. The purpose of response, then, is to interrupt and neutralize adversaries before the adversaries can accomplish their objective.

This chapter describes the process of defining PPS requirements in the DEPO process, including a detailed description of the VAI process in Section 3.1. A description of the evaluation process for a PPS is given in Section 3.2, including some of the

advantages and disadvantages of these methodologies. Information on the design of a PPS, including detection, delay and response, is available in Appendix A.

## 3.1 PPS Requirements

Before constructing a PPS, the DEPO methodology first calls for analysts to determine the objectives of the PPS system. These objectives consist of three actions [28]:

- Characterizing the facility;
- Defining the threat, and;
- Identifying targets.

For domestic NPPs, the facility characterization is largely done during the NRC license application process. Facility characterization for security applications requires collecting several items of information that describe the NPP, including siting information and operational details like hours of operation, work positions and responsibilities. Other details, such as the legal authority to use force and public support or opposition to the facility need to be collected separately to understand how the PPS can operate.

Similarly, for domestic NPPs the threat definition is largely performed by the NRC, which establishes and maintains a design basis threat (DBT) for NPPs to protect against. The DBT is a non-public document that describes the numbers and capabilities of adversaries that an NPP's PPS is expected to be able to withstand. The DBT concept is analogous to the DBA concept that establishes a bounding set of accidents that an NPP is required to consider in its safety analysis. When constructing or updating the DBT, it is

important to account for both outsiders and insiders, as well as their potential motivations. The motivations for adversaries are grouped into three categories [28]:

- *Ideological motivations*, which include people who have objections to the NPP and those who believe that their philosophical goals could be advanced through attacking the NPP;
- *Economic motivations*, such as criminal cartels that could obtain valuable material or information, and;
- *Personal motivations*, which are based in the specific conditions of individuals, such as a worker's grievance with an employer.

In addition to the motivation, the capabilities of possible adversaries are considered. One of the most important and highly considered capabilities is the number of adversaries, but others, such as weapons or tools that can be brought to bear, are also important to consider. The kind of weapons and explosives the adversary has available will greatly affect what the PPS needs to be designed to withstand. Similarly, the tools and vehicles available to an adversary have a substantial effect on the PPS design. For example, an adversary limited to hand tools and traveling on foot would be impacted by different detection and delay elements than an adversary with thermal cutting tools who travels by helicopter.

The final step in determining the PPS objective under the DEPO framework is to identify the targets within the facility. This step has three parts:

1. Determining undesirable consequences;
2. Selecting a method for target identification, and;

3. Identifying sets of targets

Domestically, the NRC has defined the undesirable consequences for NPPs. These consequences are defined as “significant core damage and spent fuel sabotage” in the NRC’s guidance [25]. Additionally, the NRC calls for protection against a release greater than the 10 CFR Part 100 limits [29] which are either a whole-body dose of 25 rem or a 300 rem thyroid dose from iodine. However, there may be other consequences that NPP operators wish to prevent (i.e., an extended shutdown of the reactor) in addition to meeting regulatory limits.

Target identification at NPPs is done through the VAI process, the steps of which were introduced in Section 2.2. The NRC guidance [20] on VAI contains some notable assumptions that differ from guidance that is more common in safety analysis. These include the assumptions that:

- No random equipment failures occur during an attack;
- “All equipment outside the protected area of the plant is lost unless continued operation of the equipment makes the situation worse,” and;
- Operator actions can only be considered under specific conditions, including adversaries being unable to interfere with the operator actions and the operators being trained to perform these actions under similar scenarios.

A detailed explanation of the steps in the VAI process is given below. The organization of the explanation is based on the VAI steps, as shown:

1. Determine inventories of nuclear material with sabotage concern (Section 3.1.1)

2. Evaluate direct dispersal as a potential risk (Section 3.1.2)

3. Identify initiating events which can lead to radiological release and systems required for mitigation of events (Section 3.1.3)

4. Construct ALM to determine combinations of events which could lead to core damage (Section 3.1.4)

5. Eliminate events from the ALM that the design basis threat adversaries are unable to perform (Section 3.1.5)

6. Identify locations within the NPP that the events remaining in the ALM can be performed and replace the events in the sabotage logic model with their corresponding areas (Section 3.1.6)

7. Solve the ALM to identify minimum target sets of areas that could lead to successful radiological sabotage (Section 3.1.7)

8. Find the Boolean complement of the target areas to produce candidate vital area sets, i.e. areas within the NPP that if all protected will prevent radiological sabotage (Section 3.1.8)

9. Select the vital area set that is most advantageous to protect (Section 3.1.9).

### 3.1.1 Determine Inventories of Nuclear Material

For NPPs, the major inventories of nuclear material are located in the reactor core, the spent fuel pools and the dry cask storage containers. However, if other locations with quantities of nuclear materials whose release might exceed the 10 CFR Part 100 limit exist, it is important that those inventories be included in the VAI.

### 3.1.2 Evaluate Direct Dispersal

For each inventory of nuclear material, the NPP should determine if adversaries within the DBT can cause direct dispersal. To do this, it is necessary to determine if the adversary has the capability to both release radionuclides into the air and to create a pathway to the environment for those radionuclides. In an NPP, the locations that contain the most nuclear material are:

- The reactor core; located in the containment structure;
- The spent fuel pool; often located in the auxiliary building, and;
- Dry fuel storage casks; located within the limited area of the site

Due to existing safety standards, these structures are built to high structural standards to protect against seismic events [30]. Containments have thick walls, built out of either concrete or steel and are designed to prevent the inside atmosphere from leaking into the environment, even at high internal pressures [31]. NPP auxiliary structures contain safety-grade equipment and are therefore built to seismic Category 1 standards. Additionally, auxiliary buildings are large, open structures and have filtration systems which can allow for radionuclides to gravitationally settle on surfaces inside the plant or trapped in the filtration systems. Dry storage casks, finally, are built with thick concrete and steel liners and can be designed to withstand strong impacts and fires. As such, it may not be credible for direct dispersal to occur, regardless of adversary capabilities.

For other material inventories, at this time a conservative analysis is performed to determine if a release of this material can exceed the release limits [20]. This analysis assumes that 100% of the material is converted into respirable particles and dispersed

into the local atmosphere, assuming a complete loss of all physical protection or mitigating systems. If, in this limiting case, the released material does not exceed the previously established consequence limits, then this material can be discounted and does not need to be considered in the rest of the VAI process [20]. Otherwise, the dispersal of the nuclear material should be considered as a possible malicious act for the remainder of this process.

### 3.1.3 Evaluate Indirect Dispersal

The indirect dispersal of nuclear material can occur when adversary-caused damage to supporting SSCs has the potential to result in a release. The damage primarily occurs as a result of potential energy within the system, such as heat or pressure, accumulating beyond the ability of the supporting SSCs to control. This can happen in two ways [20]:

- Adversaries cause an initiating event of malicious origin (IEMO) beyond those considered in the NPP's design basis, or;
- Adversaries cause an IEMO within the design basis and also damage SSCs intended to mitigate that type of event.

Notably, it is possible for an indirect dispersal to succeed without adversaries gaining access to locations containing nuclear material. It is only necessary for adversaries to access locations containing the necessary SSCs that would cause an IEMO beyond the ability of the plant to control. It is therefore necessary to determine the bounding set of IEMOs that could occur.

Many of the IEMOs are already identified in the Level 1 PRA[2], though it is possible that not all could be identified in this manner and it is therefore necessary to perform due diligence in analyzing the NPP system to identify those IEMOs that are not included in existing PRAs. These IEMOs can include IEMOs that involve passive systems that, due to low probabilities of stochastic failure, are screened out of safety risk analyses. An example could be the catastrophic loss of reactor piping systems. These systems often have low probabilities of stochastic failure and therefore may not be included in a NPP's safety PRA. However, it is still possible that an adversary could damage or destroy these systems, depending on the available tools to the adversary. In addition to IEMOs associated with low probability failures, NPPs may possess radioactive materials outside the reactor core that have not been included in PRAs, such as those in the spent fuel pool. From a security perspective, an adversary could release these radioactive materials and this release would therefore need to be added back into consideration for security analysis.

In addition to using existing risk analyses, IEMOs can be discovered through a combination of [20]:

- Referring to other VAI analyses;
- Reviewing engineering documents belonging to the SSCs that are used to maintain control of nuclear material, inside the reactor core and elsewhere, and;

[2] PRAs are divided into levels, depending on the period of an accident the analysis covers. A Level 1 PRA calculates the core damage frequency following an initial event. A Level 2 PRA starts at the onset of core damage and estimates the radionuclide release. A Level 3 PRA starts with the radionuclide release and estimates the consequences to the public [79].

- Deductive analysis, where analysts determine the functions that need to be performed to prevent an unacceptable radionuclide release.

Based on these analyses, IEMOs may be identified by considering the loss of the relevant systems.

In addition to IEMOs within the plant, it is necessary to consider IEMOs that can be accomplished from outside the plant, such as a loss of offsite power (LOOP). Such IEMOs are of critical importance because adversaries can accomplish these tasks without interacting with, and potentially being defeated by, the PPS.

If any of the identified IEMOs exceed the plant mitigation capabilities, it should be added into the sabotage logic model as a sabotage event. For those IEMOs that do not exceed the capabilities of the NPP's SSCs, mitigating systems must also be considered [20].

Mitigating systems are any system (with or without operator actions) that can reduce the effect of an IEMO and potentially prevent that event from leading to a release of radionuclides. Therefore, the VAI must consider what mitigating systems an adversary could sabotage in addition to an IEMO to affect an unacceptable release.

### 3.1.4 Develop the Sabotage FT Logic Model

Once all IEMOs have been identified, an ALM can be developed using FTs for all direct dispersal IEMOs and a number of bounding indirect dispersal IEMOs, as decided by the analyst. Since PRA makes extensive use of FTs to characterize the NPP, the ALMs developed through the VAI process make extensive use of the Level 1 PRA FTs (recall that Level 1 PRA considers safety assessments from the initiating event to the

onset of core damage). The VAI FTs have radiological sabotage as their Top Event which can occur based on a logical combination of each of the identified nuclear material inventories and the IEMOs that affect each of these inventories. The FTs are extended to determine logical combinations of systems that would need to fail in order to achieve this IEMO. For example, if an identified IEMO is a loss of Ultimate Heat Sink (UHS), then this fault is decomposed into logical combinations of systems that, if lost, would result in a loss of UHS.

While much of an NPP's ALM can be obtained from already-existing plant-specific Level 1 PRA FTs, there are differences in how both sets of FTs would be used that require modification to the PRA FT before being used in the ALM. The PRA FTs generally require that SSCs continue to be decomposed in the model until arriving at individual components whose failure probabilities can be determined. The ALM is not concerned with the probabilities of failure and does not need to model each component in the same manner. Instead, this process of decomposing the loss of a system into the logical combinations of subsystems that would need to be lost continues until the ALM has enough detail that every basic event can be identified with a specific location.

If operator actions are considered in the ALM, the operator action must meet the conditions included in the set of VAI assumptions described in Section 3.1 and the ALM should include actions where the adversary prevents the operator action from succeeding. It is not necessary to refine the ALM until it can identify the means by which each SSC can fail, as is standard in PRA FTs. Rather, it is enough to ensure that all failure modes occur in the same physical location. For example, if there are multiple ways that a pump

can mechanically fail, a PRA FT will be refined to explore each of these causes. However, if the potential pump failures are all co-located, then it is not necessary to refine the ALM in a similar way, as an adversary in the location could cause any or all of the identified pump failures. If instead some failure modes can be induced remotely, the ALM should include each remote location where failure can be induced as a separate basic event. Conversely, low-probability failures such as those of passive components, which may be possibly screened out of a PRA, are added back into the ALM as the cause of failure is adversary action.

The result of this process produces a FT that describes combinations of malicious actions that when performed lead to a radiological release. Each action, additionally, is connected to the physical locations within the NPP where it can be performed. Treating the example of the pump above as a basic action, the ALM would describe both the act of sabotaging the pump and the room where an adversary could perform this action.

### 3.1.5 Screen Out Events Beyond DBT Capabilities

At this point in the VAI process, the ALM includes all logically-sound sabotage events that could lead to a radiological release, including those which could be beyond the capabilities of the DBT adversary to achieve, and therefore do not need to be protected against by the PPS. Thus, each of the events included in the ALM are compared with the capabilities of the DBT, and those which are not credible are removed from the ALM at this time in the VAI process. Additionally, any events that are outside the capability of the PPS to prevent, such as a LOOP, that an adversary can perform outside

the NPP site boundary, are considered to occur at the most advantageous time for the adversary.

However, while some events may be outside the capabilities of the DBT, these capabilities should not be considered static. It is possible for the DBT capabilities to change, and if this occurs it is necessary to revisit this step of the VAI process and compare the events to the updated DBT capabilities. This is done in conjunction with reviewing the DEPO methodology to also ensure proper protection from the PPS.

### 3.1.6 Identify ALM Event Locations

After creating a simplified ALM, it becomes necessary to determine the areas within NPP that adversaries must access in order to achieve their goal of radiological sabotage. As some of these areas will be defined as vital areas, it is necessary to work with the PPS designers to determine area borders that can be protected to appropriate levels. Importantly, these area borders are best reduced to the minimum practicable size, as larger vital areas present significant operational and protective burdens on the NPP.

After these areas have been established, each basic event is subdivided into new basic events consisting of the locations where that event could be achieved with an *OR* gate, such that an adversary entering any of these areas would cause that event. If any of these areas are offsite, those areas are instead set to house events that are always true, representing the inability of the PPS to prevent adversaries from performing malicious actions on these events. Once this is complete, all of the bottom level events in the ALM will either be basic events representing areas within the NPP, or will be house events set to *TRUE*.

### 3.1.7 Identify Minimum Target Sets

With the ALM complete, VAI-informed target set identification can be logically solved to find minimum cut-sets of basic events. This process will result in combinations of areas within the NPP where, if single area or set of areas are reached by adversaries, enough SSCs will be damaged as to result in radiological sabotage and a release of radionuclides.

### 3.1.8 Produce Candidate Vital Area Sets

Each target set represents a single location or set of locations that adversaries can use to effect radiological sabotage. In order to protect the NPP, it is sufficient to prevent adversaries from reaching every area within all target sets. This is done by creating candidate vital area sets, which include at least one area from every identified target set. If the vital areas are all protected, then adversaries cannot sabotage a complete target set.

The final VAI FT is a graphical representation of a Boolean expression, and the mathematical theories that have been developed for Boolean algebra are applicable to FTs. Therefore, the sets of events that result in the nonoccurrence of the ALM's top event of radiological sabotage can be found by calculating the Boolean complement of the minimum target sets. The solutions to the Boolean complement are then the areas that, if not sabotaged, ensure the prevention of radiological sabotage.

While the VAI FT considers radiological sabotage, it may not be a complete representation of all vital areas; theft target sets. For example, unirradiated MOX fuel may be an attractive theft target, and areas containing this fuel should be added to all candidate vital area sets, since this is a theft target set and not a sabotage target.

Additionally, some areas in the plant are required by regulation to be vital areas, even if the ALM did not designate them those areas as necessary to protect (e.g., the central alarm station (CAS) and secondary alarm station (SAS) as called out in 10 CFR 73.55 [25]).

### 3.1.9 Select the Vital Area(s) to Protect

As all candidate vital areas are capable of protecting the NPP from radiological sabotage, the final step of the VAI process requires the NPP to decide which candidate vital area set should be protected by the PPS as vital areas. There are several logistical reasons to select one vital area set over another. Due to the level of protection of vital areas, and attendant rules such as escorting by security personnel and access control requirements, operating in or traveling through a vital area is best minimized. If it is expected that a vital area would need to be accessed during an emergency at the NPP, the extra time taken to follow these procedures would degrade emergency response. If instead the decision is made to relax access control measures during an emergency, this may degrade the PPS effectiveness and provide an opportunity for adversaries.

Additionally, in the event of an adversary attack, vital areas will be protected by the response force. If these areas cannot be safely inhabited or if the discharge of gunfire risks damaging equipment that may cause an emergency, it may be desirable to avoid protecting that area as a vital area. Beyond the safety of members of the response force, the levels of protection required for vital areas may be easier to achieve and less expensive for one vital area set than another.

## 3.2 PPS Evaluation

After a PPS has been created, the system must be evaluated to ensure that it will be effective against the DBT. This evaluation needs to ensure that all PPS elements create a system that can withstand the DBT. The probability of effectiveness ($P_E$) for a PPS is

$$P_E = P_I \times P_N \quad (1)$$

where $P_I$ is the probability of interrupting adversaries and $P_N$ is the probability of neutralizing adversaries given that they have been interrupted. Therefore, an adversary needs to be interrupted by a response force before sabotage occurs, and the adversary needs to be defeated by the response force after interruption for the PPS to be effective. The remainder of this section will describe methods used to obtain $P_I$ and $P_N$.

Analysis methods for PPSs are rooted in the concept of adversary pathways [32]. Each pathway is a set of actions that adversaries must perform in order. Once the final task is completed by adversaries, the adversary force has completed their mission. An example adversary pathway is illustrated in Figure 3-3. An important feature of this evaluation process is that adversaries can choose which pathway to take, and conservatively will take the pathway that gives them the best chance to succeed. However, adversary mission success may not necessarily follow the quickest or shortest route to a target. As a result, evaluation of a PPS examines the most conservative pathways and uses them to put bounds around the performance of the PPS.

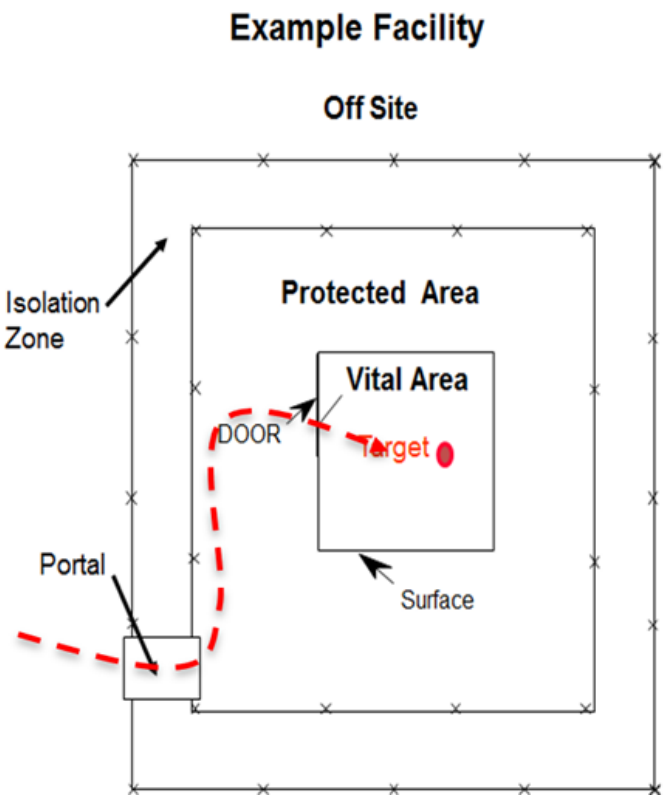


Figure 3-3 Generic example of an adversary pathway to a target [33]

The first method used to determine the effectiveness of a PPS is timeline analysis. For a PPS to be effective, it is necessary that the response timeline to interrupt the adversaries finishes before the adversary timeline to effect theft or sabotage. Additionally, delay that adversaries encounter before they are detected provides no benefit to the PPS. Therefore, the most effective strategy by adversaries would be to use stealth to bypass sensors in the PPS until detected, and then minimize the time taken to perform all remaining tasks. This strategy of using stealth until detected and then prioritizing speed both maximizes the adversary's chance to avoid detection and minimizes the effectiveness of the access delay barriers encountered. There are several performance measures that have been designed to model the behavior of adversaries.

Primary among these are the minimum time after detection point $i$ for the adversary pathway ($T_{MIN}(i)$) and the arrival time for the response force ($T_G$). If

$$T_G - T_{MIN}(i) = T_\Delta(i) > 0 \tag{2}$$

for the $i^{th}$ detection point, then it is not possible for the response force to arrive in time. If instead $T_\Delta(i) < 0$, it is possible for the response force to interrupt in a timely fashion. An illustration of this concept is presented in Figure 3-4 and Figure 3-5. Note that the response timeline in these figures does not begin when the adversary timeline does. This is because response is only engaged when on the detection of the adversary.

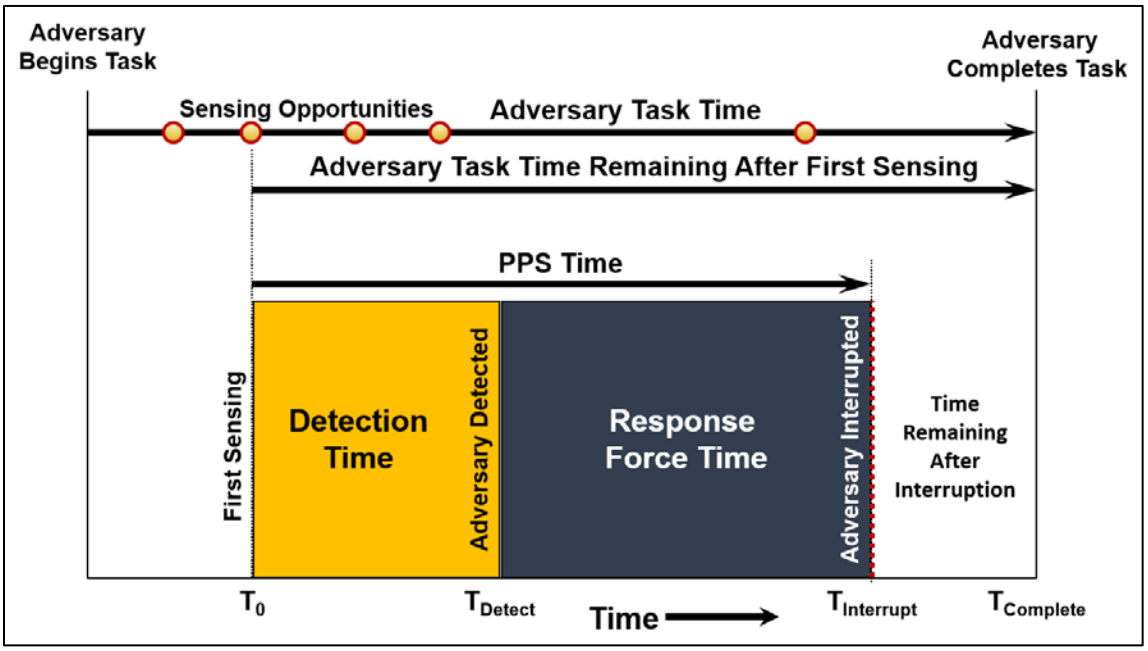


Figure 3-4 Adversary Timelines and PPS timelines, where the first sensing occurs at a timely detection point [33]

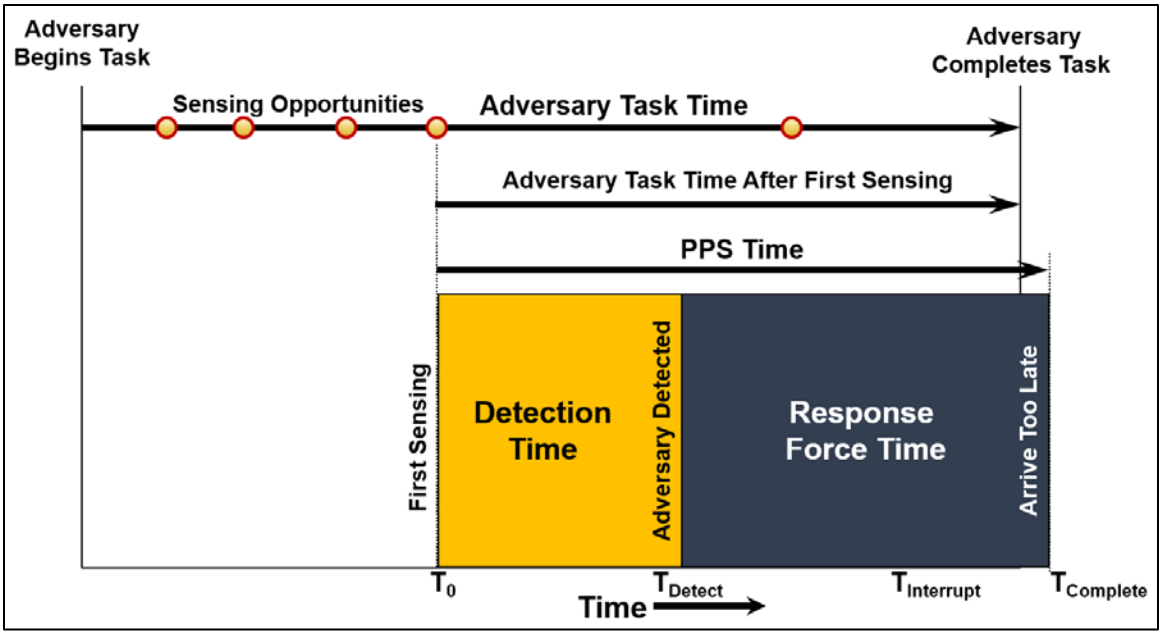


Figure 3-5 Adversary and PPS timelines where the first sensing occurs at a non-timely detection point due to late detection [33]

The calculation of $T_\Delta(i)$ in Eq.2 can be performed for every detection point *i* along the adversary pathway. Upon doing so, there will be one critical detection point (CDP) where the $T_\Delta(CDP) < 0$, but all points beyond the CDP will have $T_\Delta(i) > 0$ and the response force will be unable to respond in a timely manner (see Figure 3-5). Best practices [33] use the conservative assumption that the adversary attempts to use stealth to minimize their probability of detection up through the CDP and then uses force to minimize the time available to the response force after the CDP. If the adversary is detected at any point through the CDP the detection can then be described as timely.

Let the probability of the adversary being successfully detected at the $i^{th}$ detection point be $P_D(i)$. Therefore, the probability of the adversary being detected in a timely manner is the product of the probability of detection over every point *i* through the CDP,

designated as $k$. Note that detection which occurs beyond the CDP does not give the response force enough time to interrupt the adversary before the adversary completes their tasks. As timely detection is that which occurs in time for the response force to interrupt the adversary, $P_I$ can be recast as [33]

$$P_I = 1 - \prod_{i=1}^{k}\big(1 - P_D(i)\big), \tag{3}$$

Eq.3 shows that $P_I$is a function of the detection parameter $P_D$, and both the delay parameter $T_{MIN}$, and the response parameter $T_G$ in Eq.2. This is because $k$ is the last detection point where $T_\Delta(i) < 0$. If $T_\Delta(i) > 0$, there are three possible causes:

- Detection occurs too late in the adversary timeline (see Figure 3-5);
- Delay is insufficient (see Figure 3-6), and;
- Response takes too long to arrive (see Figure 3-7).

These issues can be resolved by moving detection earlier in the adversary timeline, adding more delay after detection, and reducing the response time, respectively. This analysis does not distinguish about which potential causes are present in the system, but it can be used by the PPS designer to decide where system upgrades would be the most cost-effective.

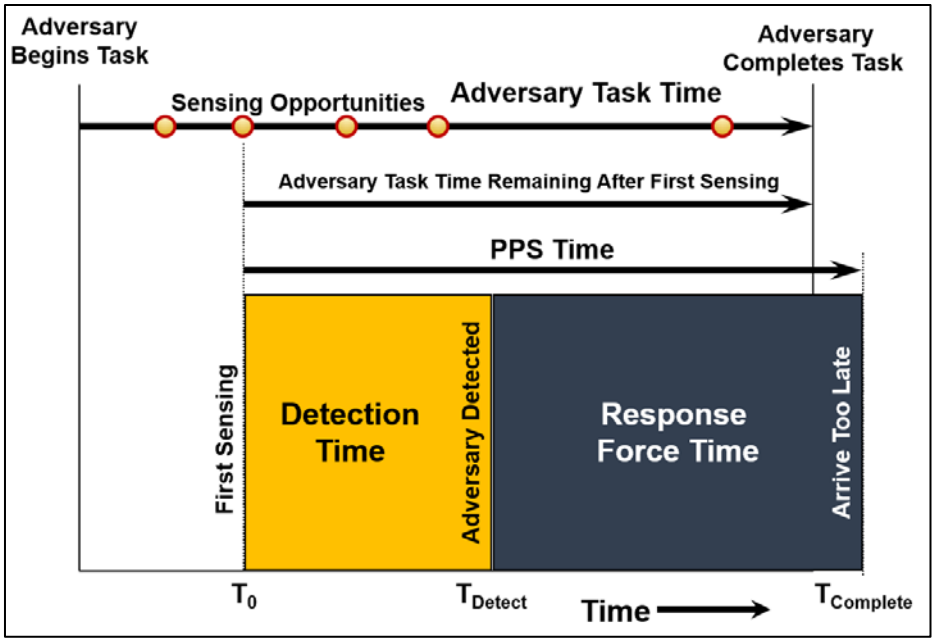


Figure 3-6 Adversary and PPS timelines where the first sensing occurs at a non-timely detection point due to inadequate delay [33]

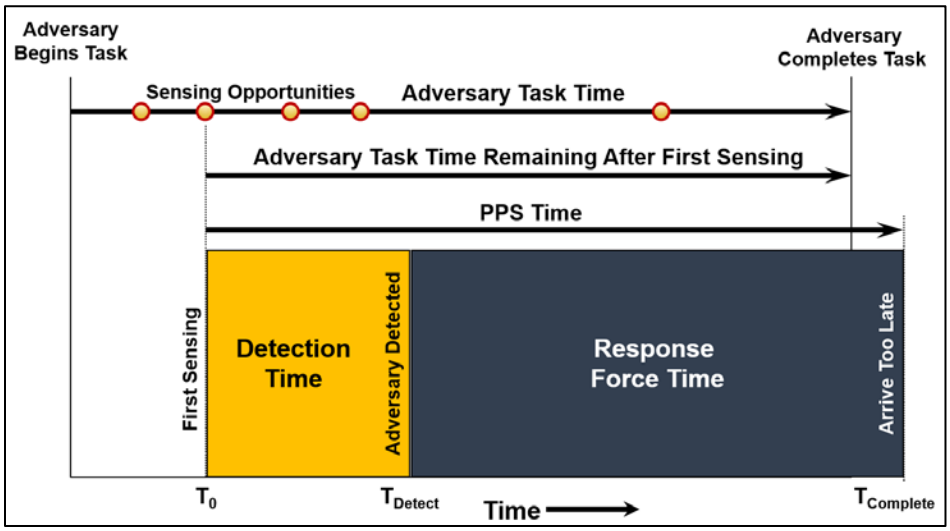


Figure 3-7 Adversary and PPS timelines where the first sensing occurs at a non-timely detection point due to slow response [33]

While timeline analysis can determine the probability for a given pathway that response is timely, it does not determine what adversary pathways are possible. Adversary sequence diagrams (ASDs) are used to categorize and identify all pathways to a single target available to adversaries. A site is divided into physical areas with protection systems between each area. All of the path elements, such as doors, walls, or other identifiable ways for an adversary to move from one physical area into another, are added to the ASD. Detection and delay values are added to the ASD for each path element. The translation process from a facility to an ASD is shown in Figure 3-8.

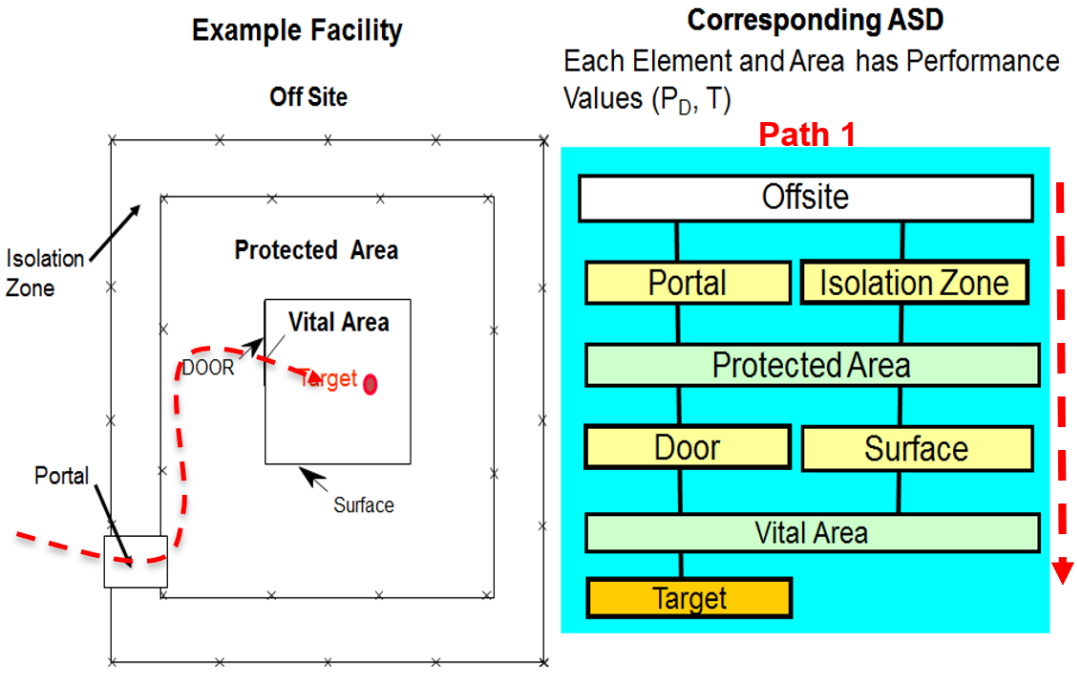


Figure 3-8 Facility layout converted to an ASD [33]

Using the ASD, each possible adversary pathway is a unique combination of path elements from the boundary of the facility to the target. Note that for sabotage analysis the ASD only needs to be evaluated for the entry path, while theft analysis requires both entry and exit paths be modeled. Theft analysis will therefore need to consider that some

barriers may have been defeated by the adversary's entrance and other barriers, such as buildings with emergency exits, have different delay times depending on the direction of travel.

Because ASDs are used to determine pathways for timeline analysis, it relies on the same assumptions used for timeline analysis. As an example, the entirety of the protected area in Figure 3-8 is one physical area and the path sequences into and out of the protected area each has one delay value which assumes that adversaries can freely travel through the protected area with no delay or detection chance. Nevertheless, the ASD can identify potentially weak paths adversaries could use for more detailed timeline analysis.

While timeline analysis and ASDs can be used to determine $P_I$, $P_E$ of a PPS requires both $P_I$ and $P_N$. Some facilities may be able to assume $P_N = 1.0$, given their DBT. For other facilities, $P_N$ is based on the response force defeating the adversaries. There are a number of methods used by facilities to model engagements between adversaries and the response force. These methods include, in increasing orders of complexity:

- Tabletop exercises (lowest cost and complexity);
- Computerized force-on-force (FoF) and pathway analysis models, and;
- Live FoF drills/exercises (highest cost and complexity).

Tabletop exercises are relatively low-cost analysis method that can be used to conduct evaluate $P_N$. While this is a versatile type of exercise, only one form of tabletop exercise will be described here. Tabletop exercises are conducted on a map of the NPP

site, and using units representing the adversaries and the response force. Analysts are divided into separate teams;

- One team controls the adversary actions,
- One team controls the response force actions, and
- One team serves as moderators and adjudicators.

This approach allows analysts to get an understanding of how the adversaries could behave and the tactics and locations of adversaries and the response force. Additionally, it allows the moderators and adjudicators to estimate $P_N$ using a combination of judgment and predetermined probabilities.

Computerized FoF models are generally similar in philosophy to tabletop exercises. However, these FoF models construct a 2D or 3D facility model and have entities (avatars) representing adversaries and the response force. FoF modeling analysts can determine the adversary pathway and capabilities, as well as the response strategy. The FoF software can be run as either with a human-in-the-loop (e.g., The Joint Conflict and Tactical Simulation (JCATS) [34] – see Section 5.1.1) or human-out-of-the-loop (e.g., Dante [35] – see Section 5.1.2). If humans are in the loop, analysts can control entities to make them react in a more realistic manner to the events that occur. However, if humans are out of the loop, the behaviors of entities are predefined based on expected conditions that could arise during a scenario. While this approach may result in more artificial entity behaviors, it allows for greater automation of the process, enabling many runs to be performed on one scenario.

Live FoF drills and exercises simulate adversary attacks on the NPP site [36]. Such drills can either be done to provide performance testing on specific PPS elements or to conduct a full-scope attack on a NPP. For performance testing, analysts attempt to defeat designated PPS elements with specified tools and collect characteristics about the effectiveness of the PPS element. For a full-scope assessment, mock adversaries develop attack pathways and conduct a simulated attack on the plant, including bypassing detection systems, breaching delay barriers, and defeating a mock response force. While these types of drills and exercise involves much of the chaos that would be expected in a real adversary attack, it is important to remember that as a simulation, it does not fully capture the behavior expected in a real attack. The process of gathering information through surveillance cannot be fully replicated, and some activities need to be simulated for safety reasons and to avoid damaging the PPS.

# Chapter 4 - Risk Analysis

This chapter introduces the concept of quantified nuclear risk and some of the analysis methods that have been used or proposed to quantify different types of nuclear risks. For nuclear safety risks, these methods include TPRA and dynamic probabilistic risk analysis DPRA. Section 4.1 introduces the concept of nuclear safety risk and use of FTs and ETs for its quantification. Section 4.2 describes DPRA methods used to quantify nuclear risk. Section 4.3 outlines the 2S interface, including areas of overlap and conflict between the two disciplines and the state of the art in conducting joint analyses.

## 4.1 Nuclear Safety Risk

A quantitative definition of risk is often described by the risk triplet introduced by Kaplan and Garrick [37]. The risk triplet is a set of three questions that are typically given as:

1. What can happen (i.e., what can go wrong?)
2. How likely is it that it will happen?
3. If it does happen, what are the consequences?

This collective set of questions divides a problem into a list of scenarios, based on all of the possible answers to Question 1. Table 4-1 provides an example of a scenario list.

Table 4-1 Generic scenario list with associated likelihoods and consequences

| Scenario | Likelihood | Consequence |
|---|---|---|
| $s_1$ | $l_1$ | $c_1$ |
| $s_2$ | $l_2$ | $c_2$ |
| $\vdots$ | $\vdots$ | $\vdots$ |
| $s_n$ | $l_n$ | $c_n$ |

Each of these scenarios $s_i$ in this table has some likelihood of occurring with probability (or frequency) $l_i$ and consequences $c_i$ in the event that the scenario occurs, forming a triplet:

$$\langle s_i, l_i, c_i \rangle.$$

If all of the identifiable scenarios are included in this list, then the nuclear risk $R$ is the set of all triplets. Formally, this is written as:

$$R = \{\langle s_i, l_i, c_i \rangle, c_i = 1,2, \dots, N\} \quad (4)$$

Practically, however, this is not possible. As mentioned by Kaplan and Garrick, a valid criticism of the risk triplet as shown in Eq.4 is that "A risk analysis is essentially a listing of scenarios. In reality, the list is infinite. Your analysis, and any analysis, is perforce finite, hence incomplete [37]." In addition to the likelihood and consequence for all identified scenarios, it is necessary to account for these scenarios that have not been identified in order to determine their contributions to the system risk. These unidentified scenarios are grouped together and collectively added to Eq.4 as $c_{N+1}$.

The risk of unanalyzed systems in NPPs can be included through conservatism. If the consequences are set to the most severe credible consequences and the probability of

their occurrence is similarly set as high as credible, then the calculated risk serves as an upper bound on the true system risk from scenarios not analyzed.

TPRA is based on ET/FT methodologies [9]. Initiating events, which involve the loss of one or more components, are logically evaluated to determine the impacts of component losses on a NPP. The FT methodology is deductive, and starts with a Top Event (TE) that the system is intended to prevent [38]. This TE has sub-events that logically combine to cause the TE. The lowest level of events are called basic events (BEs). The most common logical operators are OR and AND operators. For example, Figure 4-1 shows a FT where the TE is the output Q and the sub-events are inputs A and B. Connecting these events is an OR gate (annotated with a plus symbol). This OR gate functions in the same manner as the Boolean logical operator OR where the Q is true if at least one of A and B are true. An OR gate allows analysts to more specifically describe an event. A pump failing to work, for example, can be due to a lack of power to the pump, a failure of the pump or a loss of water to the pump intake.

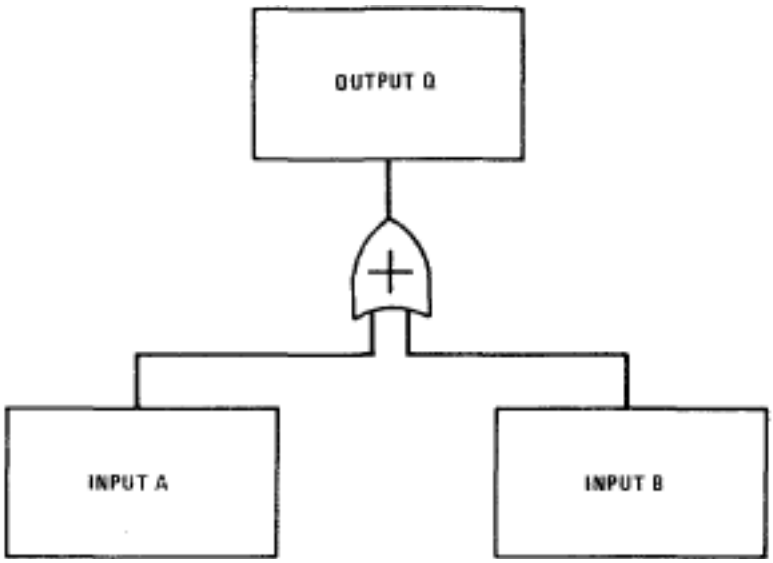


Figure 4-1 Example fault tree with an OR gate [38]

A FT featuring an AND gate is shown in Figure 4-2 (annotated with a dot). This gate functions like the Boolean operator AND in much the same way as the OR gate. However, in this case the output Q is true if both A and B are true and false otherwise. As an example, a NPP only enters a station blackout if offsite power is lost, all onsite diesel generators fail and the batteries fail. Additionally, in the event of a station blackout it can be logically assumed that all of the sub-events have occurred.

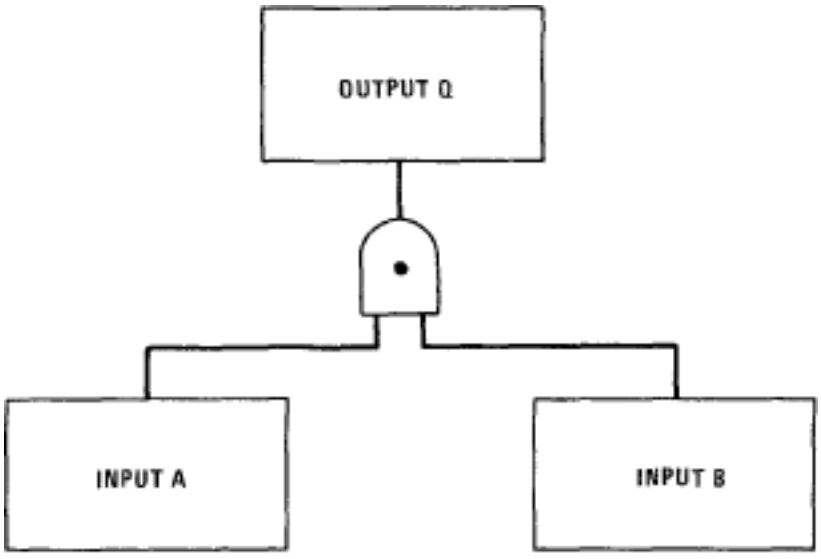


Figure 4-2 Example fault tree with an AND gate [38]

To determine the probabilities of a TE occurring, the FT must be solved. The solution process involves using Boolean algebra to find combinations of BEs that lead to the TE. Each of these combinations is a cut-set, listed by the BEs that result in the TE. Minimal cut-sets are those cut-sets where each BE is necessary for the TE, i.e. if any BE is removed from a minimal cut-set, the TE would no longer occur. When solving a FT, the minimal cut-sets are used.

ETs, shown in Figure 4-3, serve as a complement to FTs in PRA. ETs are forward looking and begin with an initiating event. Future events are then regarded as uncertain, successful or failed upon occurrence. These uncertainties, called branching points, follow the top path if successful and the bottom path if failed. This process creates a sequence of events that are mapped to a number of end states. The end states can range from “no damage” for our purposes to one of several levels and timings of damage.

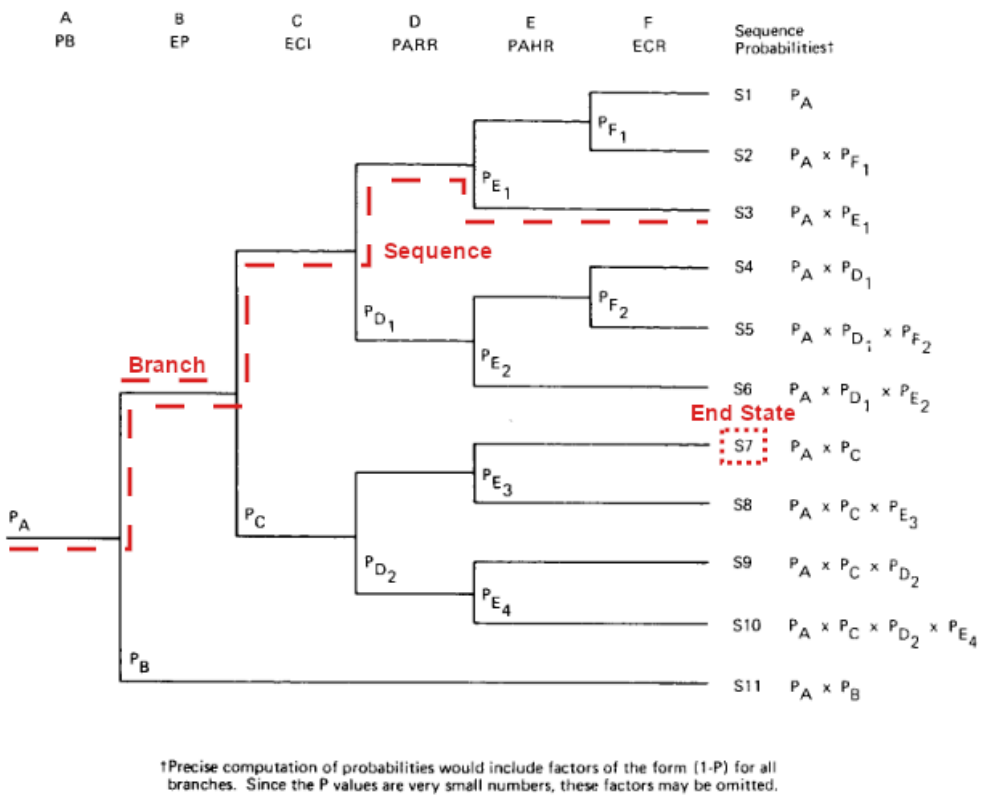


Figure 4-3 Example event tree with annotations highlighting terminology [9]

For this dissertation, the following terms (illustrated in Figure 4-3) are defined for ETs and DETs:

- *Branch*: A branch is a segment of the analysis between two branching points. During this segment, all uncertain parameters remain constant;
- *End state*: An end state is a final branch in the DET with no further branching points, and;
- *Sequence*: A combination of branches that form a continuous line from the initiating event to an end state. Note that a sequence can be uniquely defined by the values of each of the branching points the sequence travels though, in order.

To determine the probability of success or failure of each branching point, FTs are used. Each branching point is assigned as the TE of a separate FT. The basic events of each FT are assigned probabilities of occurrence and the FTs are solved to find probabilities for the branching points. These probabilities are used to determine the probabilities for each branching point in a sequence, and therefore each end state. The end state probabilities are considered, either separately or after combining similar end states, when making decisions about the risk of an NPP.

## 4.2 DETs

DETs were developed to address some of the limitations in the ET/FT methodology [2]. Here, the branching points are not determined by an analyst, as they are in traditional, or static ETs. Instead, the analyst creates a list of branching conditions (BCs) and child branches that result. A plant simulator runs using the initial state of all uncertain parameters until it reaches one of the BCs. Once a BC is reached, the simulation stops at that time, which ensures that BCs are encountered at the times and in the order that they would occur, assuming that the simulator correctly represents the system behavior. An example of a DET for a pressurized water reactor (PWR) pressurizer is given in Figure 4-4.

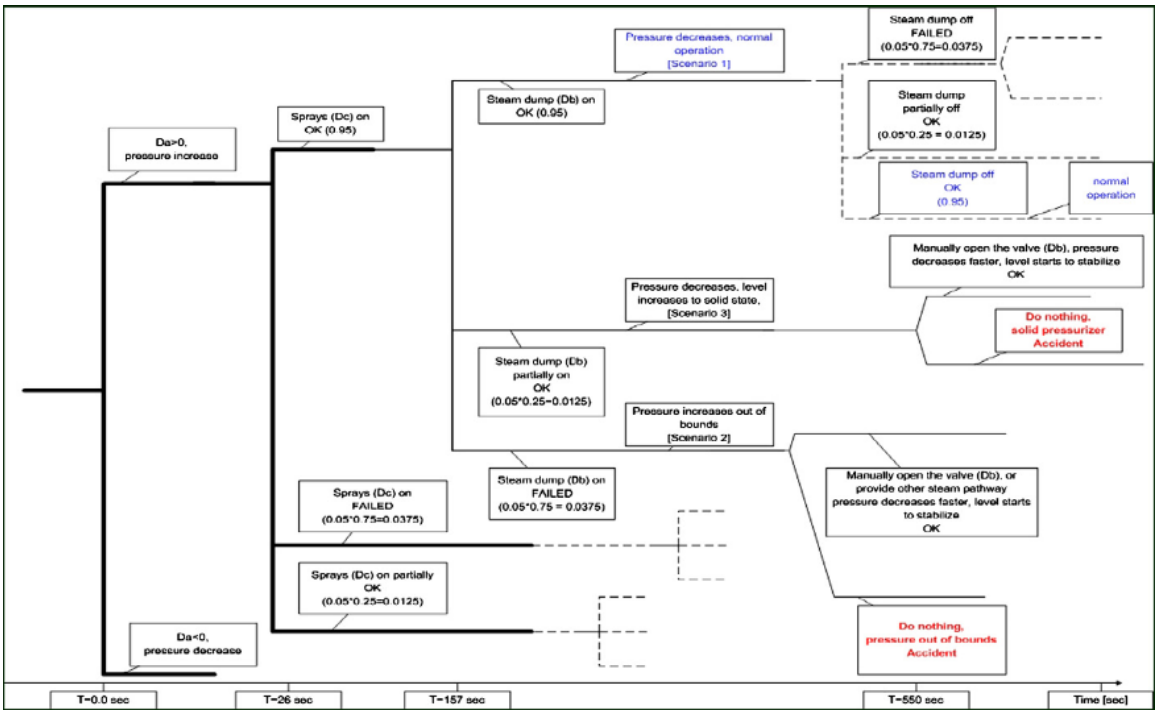


Figure 4-4 Example of a dynamic event tree for a PWR pressurizer [2]

On branching, the simulation splits into several child branches based on the BC. In a DET, there can be more than just success and failure branches. Figure 4-4 illustrates a DET with more than two child branches in the sprays BC, which occurs at 26 seconds. This BC has three outcomes: success, failure, and a degraded state. Additionally, using DETs allows BCs to repeat, occurring more than once in a sequence, which can be useful if equipment is cycling.

## 4.3 Safety-Security (2S) Interface

Nuclear safety and nuclear security have similar goals. Both safety and security seek to prevent damage to the public via the loss of service from the plant or a release of radionuclides to the environment. Many of the tools and analyses used in nuclear safety and security have parallels with the other discipline. The nuclear safety principle of a

DBA that a NPP is supposed to withstand is similar to the DBT that a NPP's security system is intended to protect against [1]. Additionally, engineered safety systems provide additional resilience against adversary attack and access restrictions to vital areas enhances safety by reducing radiological exposure to NPP workers.

Several attempts have been made to create an integrated 2S analysis by adapting various parts of either safety or security analysis to the other discipline [39, 40, 41, 42]. One of the earliest of these is VAI, outlined in Section 3.1, which adapts FTs created for safety analysis to identify vital areas in nuclear security. Similarly, the risk triplet described in Eq.4 has had several attempts to create analogous forms that are suitable for security analysis.

Another early attempt to conduct a 2S analysis was the ERDA-7 approach [43]. ERDA-7 defined risk as:

$$R = l \times c \times (1 - P_E) \tag{5}$$

where $l$ is the likelihood of an attack, $c$ is the consequences of successful sabotage and $P_E$ is the probability of effectiveness of the security system as described earlier in Section 3.2. In 2007, the U.S. Department of Homeland Security proposed a similar standard for the security of chemical facilities, based on the Risk Analysis and Management for Critical Asset Protection (RAMCAP) framework [44]. This RAMCAP framework is based on metrics of threat, vulnerability, and consequence [45]. Those metrics are analogous to those used in [37] and are intended to provide a quantitative description of security risks.

Other methods, such as the Vulnerability Evaluation Simulating Plausible Attacks (VESPA) approach [46] Risk Informed Management of Enterprise Security (RIMES) approach [43] have been proposed by researchers. Both VESPA and RIMES are security analysis methods which are scenario-based and are semi-qualitative. Each scenario is evaluated on several metrics and assigned rankings by subject-matter experts (SMEs) based on the estimated strengths of the PPS for each of these metrics. These metrics are then evaluated to calculate the security risk.

Beyond these attempts to create an integrated 2S analysis, past research has identified several areas where safety and security features can complement each other [47]. The IAEA published technical guidance on evaluating the security capability of SSCs that were installed to perform a safety function [48]. This guidance goes beyond the VAI process and calls for coordinated exercises involving both safety and security:

> "For example, an exercise scenario may simulate a group of aggressors who enter the nuclear power plant and endeavour to trigger an accident. In the first stage, crisis management will focus on security effects, but very quickly it will be necessary to consider potential safety problems arising from the attack. Special care should be taken to verify that the activities of the security forces do not jeopardize safety and that security is not needlessly jeopardized during implementation of safety measures" [48].

Methods have also been proposed which repurpose safety analyses for security [49]. Beyond VAI, which simply uses the results of TPRA as an input, there are methods that use TPRA processes in security analysis. The Bioterrorism Risk Assessment (BTRA)

method uses decision trees as a replacement for ETs [50]. Decision trees are a modification to ETs that include decision nodes, which are uncertainties based on the decisions by an entity rather than probability. Only the adversary's decisions are represented in this method by decision nodes; the defender's decisions are represented as chance nodes with associated probabilities. Here, the BTRA method assumes that adversaries make decisions which maximize the expected consequences of their actions.

Another method uses non-coherent FTs to model security scenarios [51]. A non-coherent FT is one where the failure of some component can lead to more desirable state than one where that component is working, or there is a component that has no effect on the overall system. Non-coherence arises when considering mutually-exclusive states. Security scenarios feature mutually-exclusive events when considering adversary actions. For example, an adversary can enter a protected room through a window or a door. However, if the adversaries enter the room via the door, they will not enter through the window, and vice versa. The use of non-coherent FTs allows analysts to track the probabilities of failure for a PPS and to determine the importance of various PPS components.

In addition to attempts to base security analysis off on methods designed for safety, researchers have identified NPP systems where safety and security measures are complementary [1, 52]. Such identified systems include the following:

- *Containment Structures*. These are safety structures created to serve as a barrier for radionuclides that have escaped the reactor pressure vessel. In addition to serving as radionuclide barriers, as these are strongly built structures with think

walls containment structures also serve as substantial delay barriers to adversaries [1];

- *Double Entry Doors*. These are airlock-style doors where two sets of doors need to be opened in sequence to enter. They are used to serve as a further barrier to radionuclides and to assist in maintaining negative pressure rooms, to reduce leakage. If both doors are secured, then adversaries are required to breach two sets of doors rather than one, which increases the delay [53];
- *Video Monitoring*. Video cameras are widespread in NPPs. Most of these are fixed cameras used for assessment, and some of these cameras can be controlled by security operators to perform surveillance. In addition to surveillance, the cameras can be used to monitor processes occurring in the plant to ensure that the NPP has not entered an unsafe state or to more quickly determine levels of damage that might occur during an accident[3] [53], and;
- *Passive Safety Systems*. Passive systems are those which operate without human intervention or requiring powered components such as pumps. Not only are passive safety systems not subject to human failures, but they also operate during station blackouts. As these systems are not controlled by operators, it is more difficult for adversaries to operate these systems maliciously. Additionally,

[3] However, it is important to include a word of caution here. Video cameras used for safety monitoring are often focused on different aspects of a NPP facility than those cameras used for security surveillance. Not only do the camera signals get viewed separately, but using separate cameras for safety and security may allow these separate cameras to be better focused on specific areas of interest within an NPP.

passive systems are often self-contained and continue to function unless directly sabotaged [53].

Despite the overlap that has been identified between safety and security, none of the proposed synergies represent an integrated 2S analysis method [52]. There are a number of important differences between the disciplines of safety and security that have been identified by researchers. One of the earliest identified and most critical differences is that adversaries are reasoning individuals that do not operate through chance [54]. Instead, adversaries intelligently choose strategies that they expect will be successful. Additionally, adversaries can make the decision to attack only if they believe the attack will be successful.

Because adversaries can base decisions of when or how to attack on their estimated success chances, the likelihood of an adversary attack is not independent to the consequences of that attack [55, 56, 57, 58]. Instead, attacks which adversaries predict are more likely to be successful will be more desirable to adversaries, and therefore likely to occur. Indeed, the concept of deterrence is based on this phenomenon. Deterrence occurs when a potential adversary decides not to attack a facility because the likelihood of success is perceived as being too low. This deterrence behavior can only occur if the likelihood of attack is based on the effectiveness of the PPS and the consequences of adversary success. Risk formulations similar to those in Eq.5 assume the independence of each term in the risk triplet, and therefore cannot hold for security analysis [54].

Not only are the components of nuclear security risk not independent for a NPP, but those components aren’t independent among different NPP sites. Adversaries are

often willing to attack multiple NPPs and make their decision based on the relative vulnerabilities of different NPPs [59]. If one NPP is better protected than another, an adversary is likely to choose to attack the less-protected NPP instead of the more-protected one. The likelihood of attack at an NPP is therefore not only a function of that plant's PPS, but may also be a function of other PPSs belonging to other NPPs [43].

Another difference between safety and security analyses is that PRAs are often pruned based on probability; extremely low probability events, even with large consequences, have little contribution to the total system risk. Passive components such as coolant pipes are often found to have a sufficiently low probability of failure that they can be discounted in TPRA analysis [20]. Adversaries, however, are capable of damaging SSCs regardless of their probabilities of failing. Indeed, pipes and other passive components may be easier to sabotage than large and heavy pieces of industrial equipment, depending on the capabilities of adversaries.

Finally, safety and security events do not occur under the same sets of circumstances. Nuclear accidents, especially those caused by external events, generally have initiating events occurring simultaneously. IEMOs, however, require adversaries to travel through the NPP and damage SSCs. Adversaries damage different SSCs at different times into the scenario and, if adversaries take different paths through the NPP, can damage the same sets of SSCs in a different order. The damage timing and ordering can have a substantial effect on the accident evolution.

Additionally, safety and security events have different levels of offsite response that can be available. External events are the cause of many of the design basis accidents,

but an external event is also likely to cause widespread damage to the surrounding region. Safety PRAs are designed to reflect the extent of damage that can occur during major external events; a large number of systems that are not designed to survive external events are not given credit in PRAs, and with damage to the region it may not be possible for support from offsite to arrive. For example, during the accident at Fukushima some NPP fire engines were destroyed by the tsunami and others were blocked by damage to the roads, delaying any response action involving the use of these fire engines by hours [60]. In a security event, however, the only damage a plant experiences is caused by adversaries; the NPP and surrounding area is otherwise unharmed. As such, the loss of systems that would cause core damage according to safety analysis might not cause the same level of damage through security analysis due to the effects of offsite recovery actions and available non-safety systems.

# Chapter 5 - Analysis Tools

A large number of computer codes are used for analysis of different aspects of NPPs. None of these codes are designed for both nuclear safety and security analysis. Separate codes are used for FoF analyses and to determine a NPP response to differing levels of damage. This chapter provides a high-level overview of many of the computer codes used domestically for these purposes, as well as driver codes that can be used to operate other codes dynamically. Section 5.1 covers nuclear security codes, Section 5.2 describes nuclear safety codes and Section 5.3 describes codes which serve as drivers for other codes used for NPP analysis.

## 5.1 Nuclear Security Codes

Most codes used in nuclear security are designed to perform FoF analysis which are the codes described in this section. Many of these codes are developed by the DOE, although a small number of FoF codes are developed for commercial uses. Selected FoF codes used in this discussion are the following:

- JCATS [34];
- Umbra [61] and DANTE [35];
- Scribe3D [62];
- STAGE [63];
- Simajin [64], and;

- Automated Vulnerability Evaluation for Risks of Terrorism (AVERT) [64].

### 5.1.1 JCATS [34]

JCATS is an interactive computer software tool developed by Lawrence Livermore National Laboratory (LLNL) and is used by various United States government and military security agencies to assess and/or improve security through analysis and training. JCATS is a real-time, human operated combat simulation instrument that is complementary to the other VA tools such as force-on-force exercises and tabletop analysis. Many iterations of JCATS can be conducted in a short time period without operational impact or safety concerns.

The backbone of JCATS is its robust databases that contain real-world information pertaining to elements such as terrain, munitions, sensors and weapons effects. Simulations are conducted at the entity-level, with each individual entity modeled to accurately represent the same size, weight, shape, speed and capabilities of its real-world counterparts. JCATS has multiple uses to include training and analysis. For instance, JCATS can be used by security forces trying to develop new tactics or procedures to optimize site security. Suppose a protective force wishes to gauge the effectiveness of weaponry or tactical upgrades. This is the ideal situation for the use of JCATS where a baseline adversary, adversary timeline, and current protective force attributes are used to achieve baseline simulation results. Further simulations are run with upgrades to response force (or adversary) capabilities, determining the effectiveness or ineffectiveness of upgrades.

JCATS scenarios are conducted in accordance with the SNL Warrior Code Methodology developed by the International Weapon Security, Vulnerability Assessment Team. The Warrior Code Methodology utilizes two operators, one controlling the response force, and the other controlling the adversary team. Operators are responsible for entity movement to include posture and speed, as well as weapon engagement. Response force and adversarial teams are modeled in accordance with DBT information to include force size, position, weaponry, etc.

The JCATS system allows for the replication of specific events to determine if there are trends, or if changes in compositions, weaponry, and/or tactics will alter the outcome. Multiple runs are required to eliminate one-time anomalies that can results in any stochastic process. As such, all JCATS information is thoroughly scrutinized to ensure the results reflect applicable and realistic information. JCATS simulations are structured and objective processes that ensure quality analysis and results.

### 5.1.2 Umbra [61] and DANTE [35]

Umbra has been developed by SNL to serve as a flexible tactical hybrid simulation engine and framework that can integrate physical, cyber, and behavioral elements at variable fidelity in a 3D environment. It regularly works the range of Live-Virtual-Constructive environments including faster than real time simulation calculations for generative analysis and real-time interactions that incorporate live external data feeds or human interaction.

Umbra supports a large library of existing elements, is modular, and supports reuse. A wealth of 3D geometric viewing and analysis capabilities exist. Umbra has been

used to solve specific problems itself and to develop focused applications. Initial creation of models exploring concepts in Umbra can often take only hours or days because of its ability to quickly decompose complex system problems into fundamental simulation constructs.

One uniqueness of Umbra is a formal 'Worlds Abstraction' (WA) to support modularization of any world model. This capability is in contrast to many simulation environments which rely upon a fixed set of data structures or a global variable space. Such approaches limit the practical scale and scope of problems to which these codes can be applied. Umbra uses world modules to provide realistic physical environments. It also provides event order optimization.

Agents operate in various heterogeneous scenarios that include environment (terrains, weather, plumes, communications, etc.), objects (vehicles, devices, cyber-systems, etc.), sensed phenomena (magnetic, acoustic, seismic, radiation, etc.), behavior (state based, cognitive, etc.), or external simulations as shown in Figure 5-1. These environments can co-exist in the same simulation environment and share data in a loosely coupled relationship. Due to Umbra's modular WA, it is straight-forward to combine models that use any or all of these Worlds into one functioning simulation.

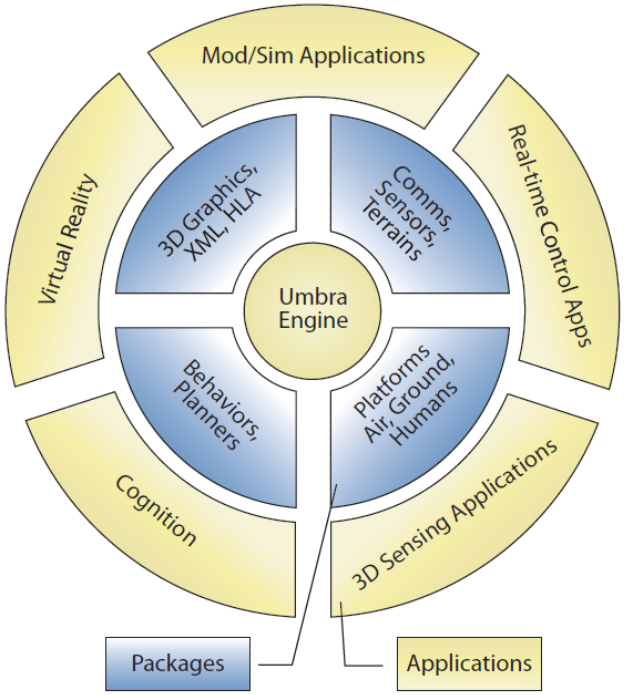


Figure 5-1 Umbra Framework

DANTE is a physical security suite built on top of the Umbra framework to perform physical security evaluation through FoF simulation. The FoF exercises that DANTE models generally involve an adversary team attempting to reach an objective location guarded by a defensive team. DANTE performs these simulations with or without human operators controlling members of either team. In DANTE, commands are reduced by the system to a set of behaviors, such as moving to a location or engaging a member of the opposite team, and these behaviors are placed in a priority queue by the DANTE simulation engine to determine the order of behaviors in this queue and update the queue as circumstances change. This system frees operators from needing to precisely control the movements of each individual entity.

### 5.1.3 Scribe3D [62]

Scribe3D is a 3D tabletop recording and scenario visualization software, created by SNL. It was developed using the Unity game engine [65] for use by other national laboratories, government organizations, and international partners. Unity is a commercial game engine built for developers and non-developers to create a wide variety of games and applications. The Unity engine features a fully customizable framework and set of development tools. Unity was used to build Scribe3D and many other training and analysis tools within the Department of Energy complex.

Scribe3D is used to create, record, and play back scenarios developed during tabletop exercises or as a planning tool for performance testing, force-on-force, or other security analysis related applications. The tools offered by Scribe3D can help facilitate open discussions and capture SME results, visualize consequences, collect data, and record events, as well as help inform decisions while users develop scenarios. Data can be viewed in 2D or 3D and played back in real-time or at various speeds. Transcript reports are automatically generated from the recorded data. The automated functions of Scribe3D allow for recorded scenarios to be run in a Monte-Carlo fashion to collect large quantities of data for analysis purposes; after initial scenarios are defined in the traditional tabletop exercise.

### 5.1.4 STAGE [63]

STAGE is a Presagis International computer code that has been further developed in partnership with SNL to provide a commercial tool for FoF modeling. Scenarios in STAGE are evaluated with computer-controlled entities that are given programmable

scripts to follow during a simulation, which can include actions such as moving to a specific location, engaging adversaries and destroying obstacles. STAGE is centered on several editors for different aspects of a simulation:

- *The database editor*, which contains all of the necessary performance data that are used in simulations, including details about the vehicles and equipment that a scenario may use, or the capabilities of the entities taking part in a scenario, such as their movement speed or ability to observe other entities in the area.
- *The mission editor*, which includes a behavioral model. This model allows the entities to automatically execute behaviors such as navigating to a specific point of interest, or automatically attempting to detect entities when appropriate, or switching between different tasks under specific conditions.
- *The script editor*, which was replaced by the mission editor and, because the script editor can run concurrently with the mission editor, now serves as a supplementary editor. This editor is currently used to model simpler and more short-term actions than the mission editor, such as determining who to shoot and what weapon to use.

Also included in STAGE are scenario and runtime editors, which determine the environment the simulation occurs in and perform the execution of the scenario themselves.

### 5.1.5 Simajin [64]

Simajin is a commercial FoF tool developed by RhinoCorps Ltd., and is used for both vulnerability assessment and “What if?” planning. Simajin simulations are driven by the Simajin Simulation Engine, which can be used for single scenarios or in a batch mode

to perform sampling. The Simanij tool is used to generate scenarios for Simajin, and uses text template files to construct a graphical user interface (GUI) for scenario generation. Simajin can also be operated on the command-line instead of through the GUI, if desired.

### 5.1.6 AVERT [64]

Ares Security Corporation produces the AVERT code, which is used by nuclear facilities and the NRC. This code is divided into multiple packages. The most basic is the AVERT Core, which is the foundation of the AVERT toolkit. This package is used for model construction and is capable of driving a batch of simulation for a given scenario of interest. There are additional packages which can be added onto the AVERT Core package, depending on needs:

- *AVERT Physical Se*curity adds an Advanced Behavior Module to represent the actions of adversaries and response forces. Additionally, this package includes a Simulation Controller module, which is used to generate multiple scenarios and run each in series. The results of these simulations are handed off to a database which provides the information for necessary post processing.
- *AVERT All Hazards* incorporates the physical security package and adds additional behaviors corresponding to natural disasters, including fire, wind, flooding and seismic events. The Simulation Controller module for *AVERT All Hazards* is upgraded to accommodate these additional behaviors and scenario types.

## 5.2 Nuclear Safety Codes

Nuclear safety analysis makes use of several models and simulations that analyze the evolution of accidents in a NPP. DPRA, specifically, requires the use of a system

response code which models a nuclear reactor from the time of an IE through the onset of core damage to determine the extent of damage which occurs. Selected system codes which perform this function are:

- MELCOR [3];
- the Modular Accident Analysis Program (MAAP) [66], and;
- RADTRAN [67]

### 5.2.1 MELCOR [3]

MELCOR is a severe accident analysis code produced by SNL. This code is widely used to evaluate reactor accidents, including by the NRC, and can model accident evolution from an initiating event through the release of radionuclides to the environment. Modeling capabilities include decay heat generation, coolant flow, reactor damage and fuel melting.

MELCOR uses a system of packages to model different effects within a NPP. The flow of fluids through the plant, including gases and liquids, is performed through the control volumes (CV) package. The CV package uses the temperatures and pressures of fluids as well as connections between different CVs to calculate the fluid flow. Solid structures in an NPP are modeled in the heat structures package. This package is used to track heat transfer through the solid structures in the plant, such as from the reactor pressure vessel to the containment atmosphere. Additional packages that are used to model more specialized phenomena include the COR package, which models the reactor behavior in the core region of the reactor in greater detail. Other packages model core-

concrete interactions and track radionuclides traveling through the NPP and into the environment, if necessary.

A MELCOR analysis is based on two codes: MELCOR and MELGEN. MELGEN is used to create a MELCOR analysis. This code creates the reactor structure and initial state, which are saved as a *restart* file. MELCOR loads a *restart* file and tracks the system evolution. MELCOR is additionally able to modify the reactor model in limited ways, which allows MELCOR to model and track damage. Modifying a MELCOR input file changes the reactor structure on loading a *restart* file.

### 5.2.2 MAAP [66]

MAAP is a severe accident code created by the Electric Power Research Institute. This code sees widespread use by the domestic NPP fleet to model the evolution of transients in NPPs and to support PRAs. Additionally, MAAP is used by NPP operators to evaluate severe accidents to support ongoing license renewal applications. MAAP was also used to support post-Fukushima activities understanding how accidents progress.

MAAP is designed to support specific reactor designs. There are separate versions of MAAP for different reactor designs, including:

- PWRs;
- Boiling Water Reactors (BWRs);
- the Russian Pressurized Light Water Reactor (VVER);
- the Canadian Pressurized Heavy Water Reactor (CANDU), and;
- Advanced Thermal Reactors (ATR).

While MAAP is only used to support specific reactor designs rather than being generally applicable to all reactor designs, reactor specific versions of MAAP use tabularized results and takes advantage of previously determined correlations. By looking up tabularized results rather than always needing to calculate effects, MAAP is able to run several orders of magnitude faster than real-time.

### 5.2.3 RADTRAN [67]

RADTRAN is a lightweight code developed by SNL in 1977 to analyze the risks and potential consequences of transporting nuclear material. There are two cases considered by RADTRAN: routine transportation and accidents. During routine transportation, nuclear material emits radiation to the surrounding environs through whatever shielding is in place. A shipment is tracked through a route, including during stops to refuel or for a driver to rest, and the dose to the public is calculated based on the time the shipment takes and the population density along the route. In addition, doses to people who might be in close proximity to the nuclear material, such as inspectors and the drivers, are modeled.

Transportation accidents are also modeled. During an accident, the package nuclear material is shipped in can become damaged, which can either reduce the amount of shielding or provide a pathway for radioactive material to be dispersed from the package. Dispersed material can contaminate the surrounding environment and nuclear material in a damaged package can irradiate the populace until the material can be repackaged and moved.

## 5.3 DPRA Tools for NPPs

In addition to codes used specifically for security or safety analysis at NPPs, codes have been developed to support DPRA for NPPs. These codes manage the dynamics of NPP transients and can drive other tools which model specific phenomena. Some of the DPRA tools that have been developed are:

- ADAPT [68];
- DYLAM [69];
- MCDET [70];
- ISA [71];
- ADS-IDAC [72], and;
- EMRALD [73]

### 5.3.1 ADAPT [68]

ADAPT, developed by The Ohio State University for SNL, is designed as a driver of system codes. ADAPT consists of several packages, including *ADAPT Server*, *database*, *editrules* and *wrapper* files. *ADAPT Server* is the package that manages the backend of DET analysis. Management includes the job-scheduling task for HPCs, as well as transferring information from one branch to daughter branches. The ADAPT Database manages the data after it has been collected and can be interrogated to group data based on how the plant responded to specific points of uncertainty. In order link a new simulator (or combination of simulators) the user needs to create a new *wrapper* file. Additionally, to perform any ADAPT simulations, the user needs to create an *editrules* file which describes the uncertainties and how they are resolved.

Generally, to link a simulator to ADAPT the simulator must meet a set of basic requirements. These requirements are that the simulator must [1]:

- Stop on system values crossing a pre-defined threshold;
- Stop on command from ADAPT;
- Output the reason for any code stoppage, and;
- Restart using modified system parameters

In order to link a code which meets these requirements, a *wrapper* file must be made. This *wrapper* contains instructions for ADAPT to perform for each branch. At a minimum, this includes the instructions to execute the simulator or simulators for one branch of an experiment. These simulators will have one of three possible outcomes:

- The simulator could stop at a BC;
- The simulator could reach the simulation end time for the experiment, or;
- The simulator could fail.

If the simulator stops due to a BC, it is required to report a code corresponding to the BC that was reached. This code is given to ADAPT and matched up with the *editrules* file to determine what variables need to change for daughter branches that are produced, including determining which simulator is supposed to be executed next. The necessary simulator files are handed off from the parent branch to its daughter branches and the wrapper ends. *Adapt-server* then performs the necessary job scheduling to execute the daughter branches. Figure 5-2 illustrates this process.

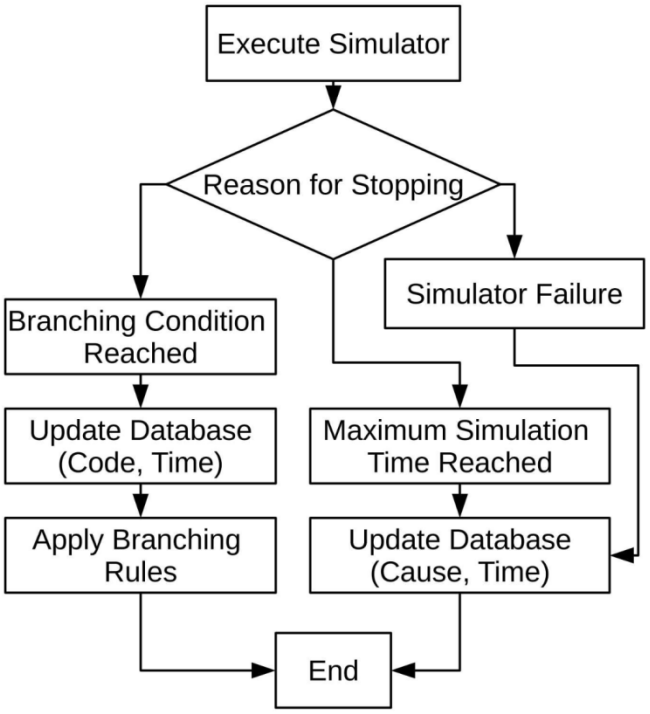


Figure 5-2 ADAPT wrapper behavior

Currently, there exist no computer simulators which model a FoF engagement and an NPP system response. As such, any DET that combines safety and security needs to be compatible with multiple simulators. In 2016, ADAPT developers updated the code to accommodate branching among simulators when necessary.

Originally, ADAPT's branching process created an input file from a template input file, incorporating the effects of all previous branches. After the upgrade, the ADAPT branching rules were modified to allow the analyst to assign one template input file for each simulator [5]. In addition, at each BC, the analyst is required to specify which simulator is run by ADAPT for the next branch. A diagram of the updated multi-simulator ADAPT branching process is illustrated in Figure 5-3.

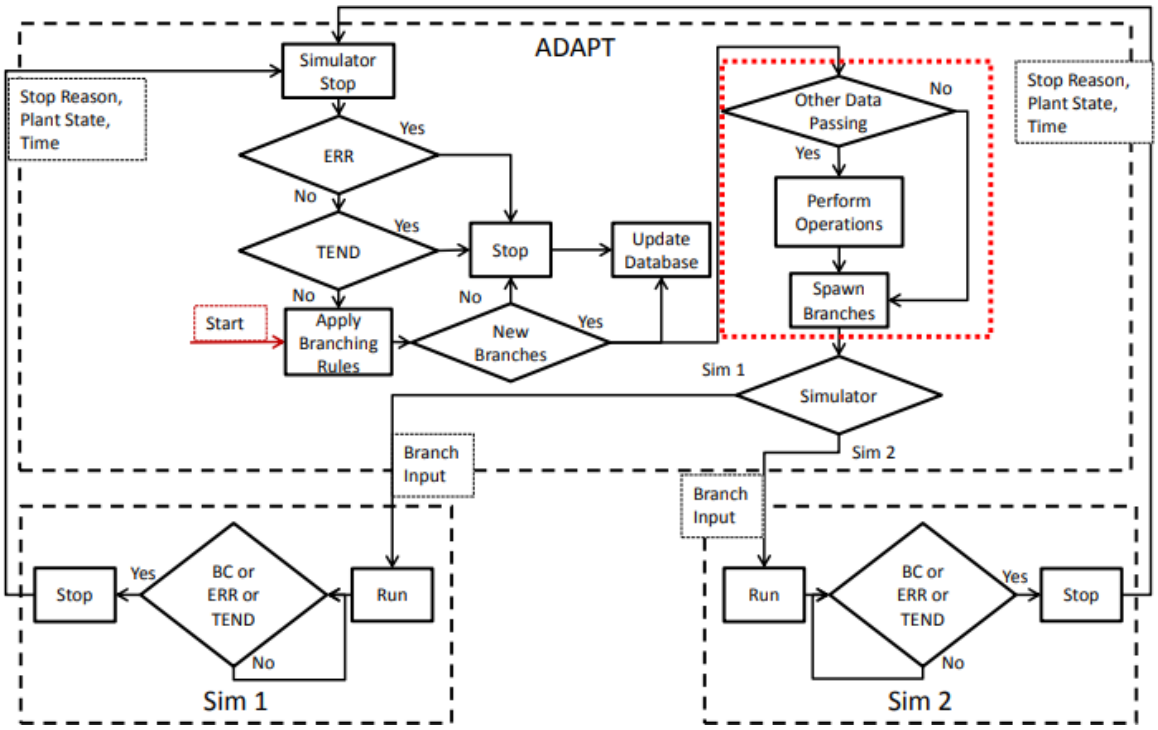


Figure 5-3 Multi-Simulator ADAPT branching process

This new formulation of ADAPT was created to allow DETs to be used in cases where a secondary simulator can be called to model specific phenomena that the primary simulator is unable to capture adequately, in order to drive the overall system evolution.

### 5.3.2 DYLAM [69]

DYLAM is an early DET code, dating back to the 1980s. This code drives a physical simulation using fixed time steps. There are six probabilistic options available to the user. Among these options are stochastic transitions, where at each time step there is some fixed probability that components in the physical simulation will move to a different state. Another primary option is to use functional dependent transitions, where components change among states with probabilities that depend on the physical

parameters of the system. The new state that a component transitions to may be a failure state or one of several degraded states. The additional fidelity in component states, along with tying these state changes to explicit times, allows for DYLAM to supplement traditional PRA approaches.

### 5.3.3 MCDET [70]

MCDET is a DET code that also uses Monte Carlo sampling, depending on the type of uncertainty to model. If a given uncertainty can occupy discrete values, MCDET uses the possible values of this variable as BCs for a DET. If instead a variable is continuous, MCDET performs Mote Carlo sampling on this variable. The combination of these two approaches leads to a random sample of DETs. The evaluation of these sets of DETs can be used to get an approximation of the uncertainty space of the modeled system.

### 5.3.4 ISA [71]

The ISA methodology is a DET process that is built using information from existing traditional PRA ETs. These existing ETs are collected and used to create generic ETs which cover the full range of the phenomenon in question. DETs are constructed with branching criteria based on the traditional ETs, and then grouped together into a single DET. The ISA process uses this DET to determine the sequences of interest, which are those sequences where the level of damage depends on an uncertain parameter of interest. The parameter of interest is sampled on and explored for the sequences of interest to get an understanding of where the system transitions from success to failure

within the uncertainty space. A schematic outlining the ISA process is given in Figure 5-4.

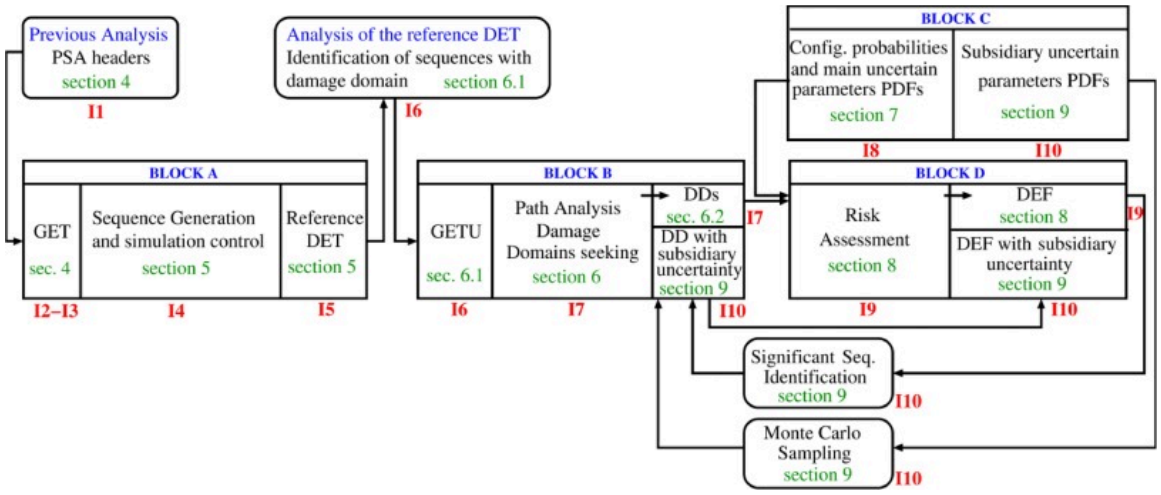


Figure 5-4 Schematic of the ISA methodology process [71]

### 5.3.5 ADS-IDAC [72]

ADS-IDAC is a DPRA code that is a combination of the ADS and IDAC codes. These two codes are directly integrated to incorporate human modeling into accident scenarios. ADS-IDAC uses a DET structure with several modules representing different elements of a plant. These elements include the crew module which models human behavior and an indicator module which represents the control panel in a NPP. The scheduler module controls the system sequence and the DET performance.

At each time step in ADS-IDAC, the ADS model updates the physical status of the plant and passes the necessary information to the IDAC code, which models crew behavior. In this way, if either ADS or IDAC reach a BC, the other model receives that information immediately and can incorporate the necessary changes. This process is shown in Figure 5-5.

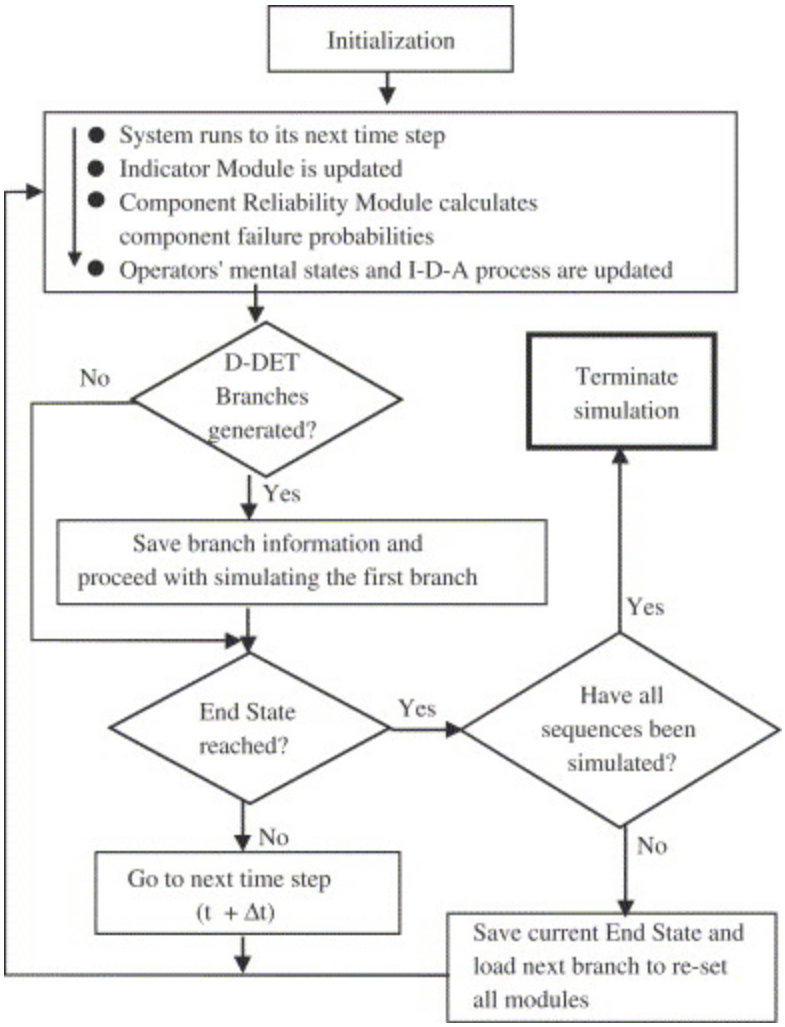


Figure 5-5 ADS-IDAC branching diagram [72]

### 5.3.6 EMRALD [73]

EMRALD is an Idaho National Laboratory risk modeling tool which is based on Markov processes. EMRALD is designed to have a similar feel as traditional PRA. Markovian states are used to model specific systems instead of event trees and connected to fault trees which are used to track interdependencies among systems. EMRALD states are based on the Three Phase discrete event process, as shown in Figure 5-6.

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

1. While there are States in the New Sates list, For each State :
   - Add the Events to the Time Queue or Conditional 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).

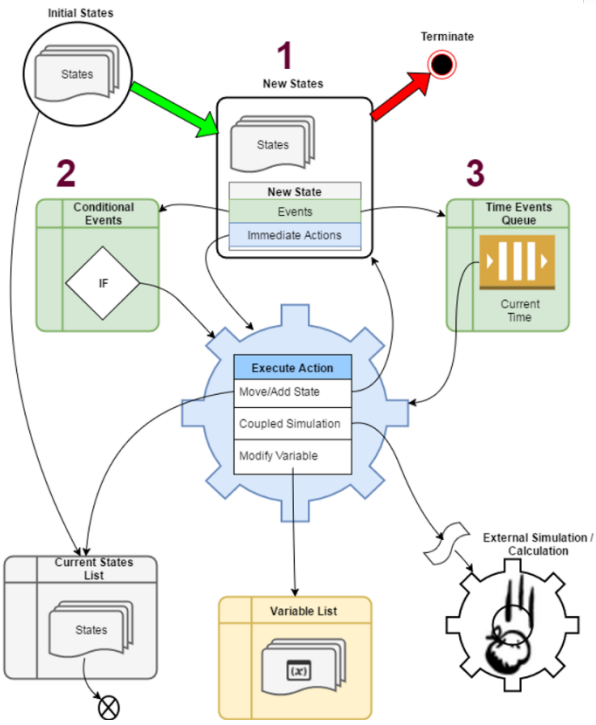


Figure 5-6 EMRALD three phase discrete event process [74]

The three phase discrete event process allows EMRALD to base probabilities on events that occur within one simulation. For example, the failure rate of a valve can depend on the time that valve opens within a simulation. Additionally, looping actions can be easily implemented using Markovian states. Additionally, certain states are designated by the analyst as key states, representing events such as core damage. These key states are collected by EMRALD for each run and reported as results of the EMRALD simulation.

# Chapter 6 - Methodology

To address some of the challenges in security analysis, described more fully in Section 4.3 it may be possible to take advantage of additional insights that could be gained from safety analysis of nuclear plants. VAs are intended to determine the risks to a NPP from theft and sabotage, and calculate the effectiveness of the physical protection system, which target sets are lost in the event of successful adversary sabotage and the timing of sabotage. By using DETs rather than ETs, safety analyses of nuclear plants are able to capture dynamics in systems that have been found to be difficult to model otherwise. As outlined in Section 4.2, DETs use a system model to capture the time-dependent system evolution while performing the analysis. Depending on the system, the behavior of that system may be highly sensitive to the uncertainties. For example, in a security event, the time between reactor scram and radiological sabotage can be defined as the variable $\Delta t_{sc}$. The realized value of $\Delta t_{sc}$ can have a significant effect on the decay heat that needs to be removed and therefore the consequences of successful sabotage. Capturing this behavior using ETs would require constructing large ETs and potentially needing to construct a new ET for each realization of $\Delta t_{sc}$, as different systems may engage or may engage in different orders based on $\Delta t_{sc}$. However, each branch of a DET relies on simulation of the system model and thus would be able to capture the effects of variations in $\Delta t_{sc}$ on the DET structure.

In addition, ETs consider the time of a scenario implicitly while DETs model time explicitly. As such, in the joint safety-security space, DETs are more easily integrated with the explicit time parameter used in VAs. To combine an explicit-time VA with an ET, it is necessary for the analyst to interpret the events in the safety ET and the security VA and reconcile the event ordering. Reconciling the time and order of events in this manner for ETs likely would require a great deal of judgment from multiple experts and may not be consistent among analysts. Additionally, since security events can evolve rapidly over the course of seconds or minutes, it may not be possible for experts to determine events within the plant to such a high resolution. However, as the time to branch for DETs is determined by phenomenological models that commonly include an explicit time parameter, that time can be reported and used to determine the event ordering.

As illustration of a possible linking process for a safety code and a security code (Case Study 1) is presented in Section 6.1. This case study demonstrates the limitations of current DET capabilities when using multiple simulators in one analysis as stated earlier in Section 1.3. Following this case study, the novel leading simulator/trailing simulator (LS/TS) methodology is introduced in Section 6.2. Section 6.3 (Case Study 2) demonstrates the feasibility of the proposed LS/TS approach on a simple system.

## 6.1 Case Study 1: Spent Nuclear Fuel Transportation Scenario

As part of a larger analysis into integrated safety, security and safeguards risk assessment [75], a case study using DETs was performed. The study hypothesized a multi-modal spent nuclear fuel (SNF) shipment across state lines. Using this shipment as

a scenario, the safety, security and safeguards risks were jointly considered to identify risks that crossed between these traditionally separate disciplines. Within the scenario, the DET case study used ADAPT to connect safety risks with attendant security risks.

In this hypothetical scenario, the State of Zamau uses nuclear power for a significant percentage of its electricity needs. It operates a NPP and has an agreement to send its SNF to the nearby State of Kazneera, which operates a commercial SNF repository. Between those two states is the State of Famunda, which operates no nuclear facilities of its own. All three States are signatories to the Treaty on the Non-Proliferation of Nuclear Weapons.

A SNF shipment, as part of the agreement between Zamau and Kazneera, takes the following route as shown in Figure 6-1:

- SNF cask is loaded at the origin facility (Site A) onto a rail car for transportation to the Port of Zamau (straight grey line in Figure 6-1);
- SNF cask is transferred from the rail car to a barge at Port of Zamau;
- SNF cask travels via international waters to the Port of Famunda (curved blue line in Figure 6-1);
- SNF is transferred from the barge to a truck at Port of Famunda;
- SNF cask travels by truck to the Famunda/Kaznirra border crossing (straight orange line in Figure 6-1); and
- SNF continues travelling by truck to the destination facility (Site B) in Kaznirra (curved orange line in Figure 6-1).

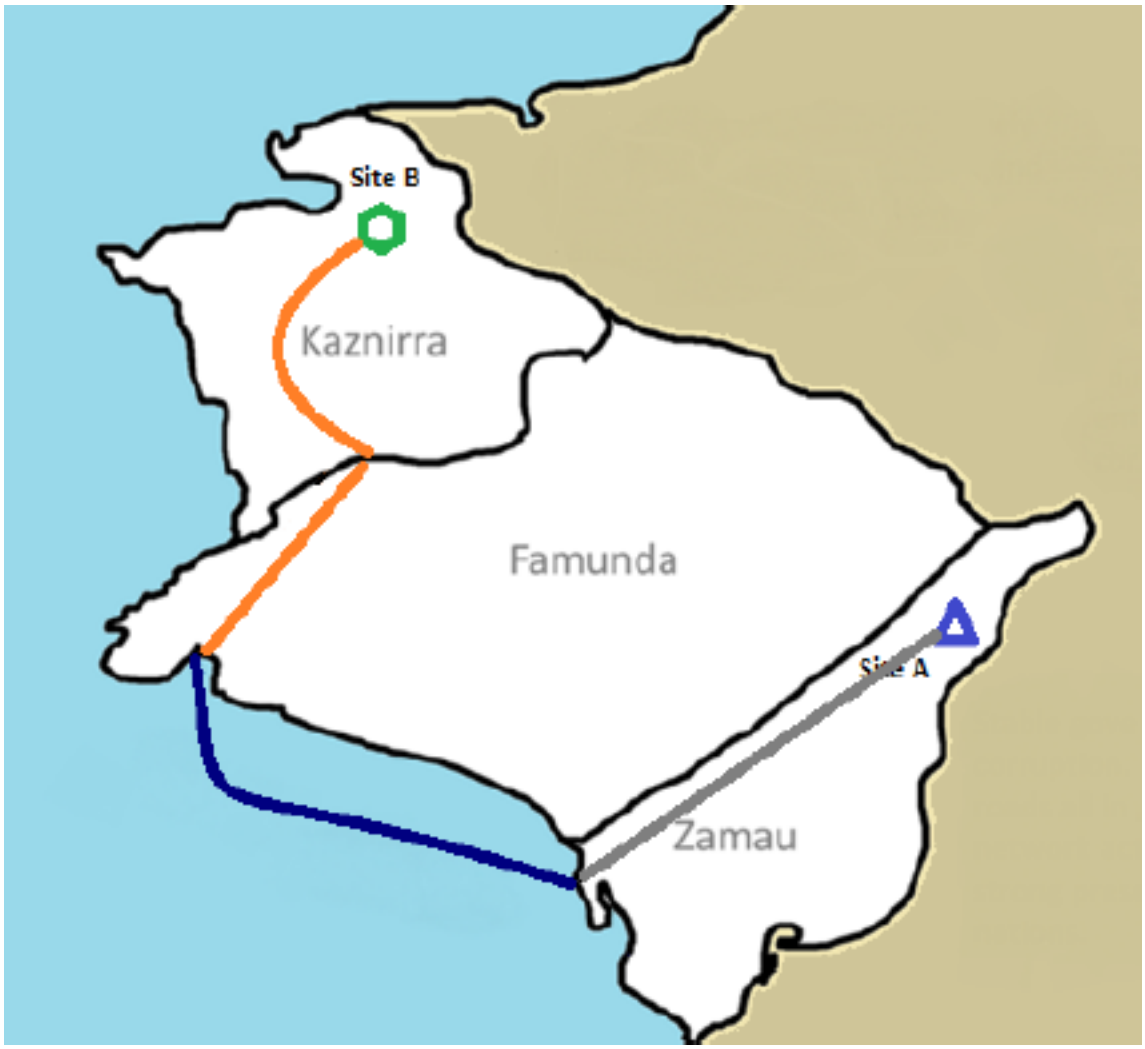


Figure 6-1 SNF shipping route in Case Study 1

Case Study 1 developed a combined 2S scenario involving the derailment of the train in Zamau due to a missing 40-ft stretch of track, after which the train was attacked by adversaries attempting to effect a release of radionuclides or steal SNF. A response force traveling with the shipment engages with the adversaries to prevent the theft or release.

The train is six cars in length and operates as a dedicated shipment. Behind the locomotive is a carriage containing half of the dedicated response force. The third through fifth cars are the SNF cask and empty buffer cars on either side of the cask, to increase the distance between the SNF and occupied rail cars. The final rail car is a second carriage containing the other half of the response force.

### 6.1.1 Linking

To perform the DET analysis for Case Study 1, appropriate ADAPT files needed to be constructed, the most important of which being the *wrapper* and *editrules* files. The *wrapper* file was created to allow for the joint operation of STAGE and RADTRAN, and could be reused for other analyses using the same simulators. RADTRAN was chosen as the case study models a transportation event, and STAGE was chosen to model the security aspects of this scenario. The *editrules* file is specific for this scenario and describes the branching that occurs within this scenario. The *editrules* file for Case Study 1 can be found in Appendix B. This linking process for ADAPT is illustrated in Figure 5-3.

Using ADAPT, it is possible to modify an arbitrary number of input files for different simulators due to a single branching condition, allowing for complex relationships between different stages of an analysis, as described in Section 5.3.1. For Case Study 1, BCs were created to modify two codes. Some conditions modify one of the two codes, such as the potential discovery of track damage, which modifies the RADTRAN input files (although this branching leads to follow-on effects that modify the probabilities and potential states of analysis by the other codes). Some modify multiple

simulators, such as branching on the accident severity. This BC affects the radioactive release in RADTRAN, the number of available response forces, and the ability to access the cask in STAGE. Table 6-1 summarizes the different BCs included in Case Study 1 and their effects.

Table 6-1 List of RADTRAN-STAGE branching effects

| **Branching Condition** | **RADTRAN Effects** | **STAGE Effects** |
|---|---|---|
| Cask Inventory: Burnup, Age | • Alters public consequences in the event of a release | — |
| Degree of Notice Given to Local Law Enforcement (LLE) | • Reduces public evacuation time in the event of a release | • Shortens time of arrival for offsite reinforcements<br>• Potentially increases ability of adversaries to gather and plan, due to leaks of route |
| Discovery of Damage to Track | • Allows for the train to either reduce speed or change route to avoid damaged track | — |
| Severity of Derailment | • Increases release to the environment | • Reduces the number and readiness of available response forces due to injury<br>• Increases the amount of time necessary for adversaries to arrive at the SNF cask due to wreckage |
| Size of Attack | — | • Affects the number of adversaries |
| State or Major Non-state Actor Sponsorship of Attack | — | • Sponsorship of attack allows for better equipment and additional adversaries |

For this case study, branching occurred in chronological order for ease of understanding. As such, the DET analysis was separated into two phases. Phase 1 used RADTRAN to model the safety consequences of the scenario during the derailment event, and Phase 2 used STAGE to estimate the probability $P_N$ of neutralizing adversaries following a derailment. This is an artificial construct of the scenario, and is only effective because the scenario can be broken cleanly into separate phases in this manner. As each branch retains the conditional probabilities for previous branches and is assigned a conditional probability in the *editrules* file, the overall probability of a branch is calculated based on the probabilities of all preceding branches.

### 6.1.2 Results

Case Study 1 combined RADTRAN and STAGE simulations to model the evolution of the scenario through links between the two codes. In total, 33,681 total branches were examined during the analysis, with more than 20,000 terminal states. The analysis calculated the radioactive release doses from a derailment accident in RADTRAN, as well as the attendant probabilities of a successful attack by an adversary directly following the derailment in STAGE. At each terminal state, the adversary won if they defeated the response force (including offsite responders) or had uninterrupted access to the SNF cask for long enough to breach the cask walls and release the loaded SNF. If all adversaries were interrupted and neutralized before completing their objectives, the responders won.

The dose released in Phase 1, as the maximum exposed individual, is given in Table 6-2[A]. Dose calculations depended on the size of the accident, which affected the

release fractions, and the advanced notice given to LLE, which affects the evacuation time for nearby members of the public. In Phase 2, $P_N$ is the metric of interest. This probability was conditioned by the events in Phase 1, such as the size of the derailment. The conditions in Phase 2 include state sponsorship of the attack. Table 6-2[B] illustrates $P_N$ for the overall scenario.

Table 6-2 Combined RADTRAN-STAGE scenario output measures.

| | | Output Measure | |
|---|---|---|---|
| | | [A] Maximum Individual Dose (rem) | [B] $P_N$ |
| Scenario | Full Scenario | 82.09 | 65.91% |
| | Advanced LLE Notice | 81.36 | 72.38% |
| | Minimal LLE Notice | 82.82 | 59.46% |

$P_N$: probability of neutralizing adversaries following a derailment

Table 6-2 shows the averaged maximum exposed individual dose consequence and the probability of neutralization given the decision to provide advanced notice of the SNF transport to LLE. Providing advanced LLE notice has several effects on the scenario. These effects are:

1. Decreasing the public evacuation time;
2. Reducing the offsite response time, and;
3. Increasing the potential number of adversaries.

Note, however, that as the BC on providing LLE notice is weighted equally between both child branches, the results for the full scenario are the mean of the results from advanced or minimal LLE notice.

By performing DPRA branching and tracking the conditional probabilities, this analysis was able to explore the full system space in a manner amenable to analyzing specific events during the scenario. For example, one BC is on the degree of advanced notice given to LLE. To determine the effects of giving more information to LLE, it is not necessary to create models of the scenario for each related possibility. Instead, calculating the conditional probability of the branches that descended from more advanced notice in comparison to the conditional probability of the branches that descended from minimal notice showed the importance and effects of this particular branch. An excerpt of the DET branching structure used in Case Study 1, including LLE notice, is shown in Figure 6-2.

Interrogating the results highlighted one interesting interaction between the safety and security analysis: that of hazards around the cask making it more difficult to access. An additional delay in breaching the cask applied to the adversaries represented the difficulty in accessing the cask. In other words, the additional wreckage and fires resulting from the derailment corresponded to making accessing the SNF cask more difficult and provided offsite responders additional time to arrive for interruption and neutralization.

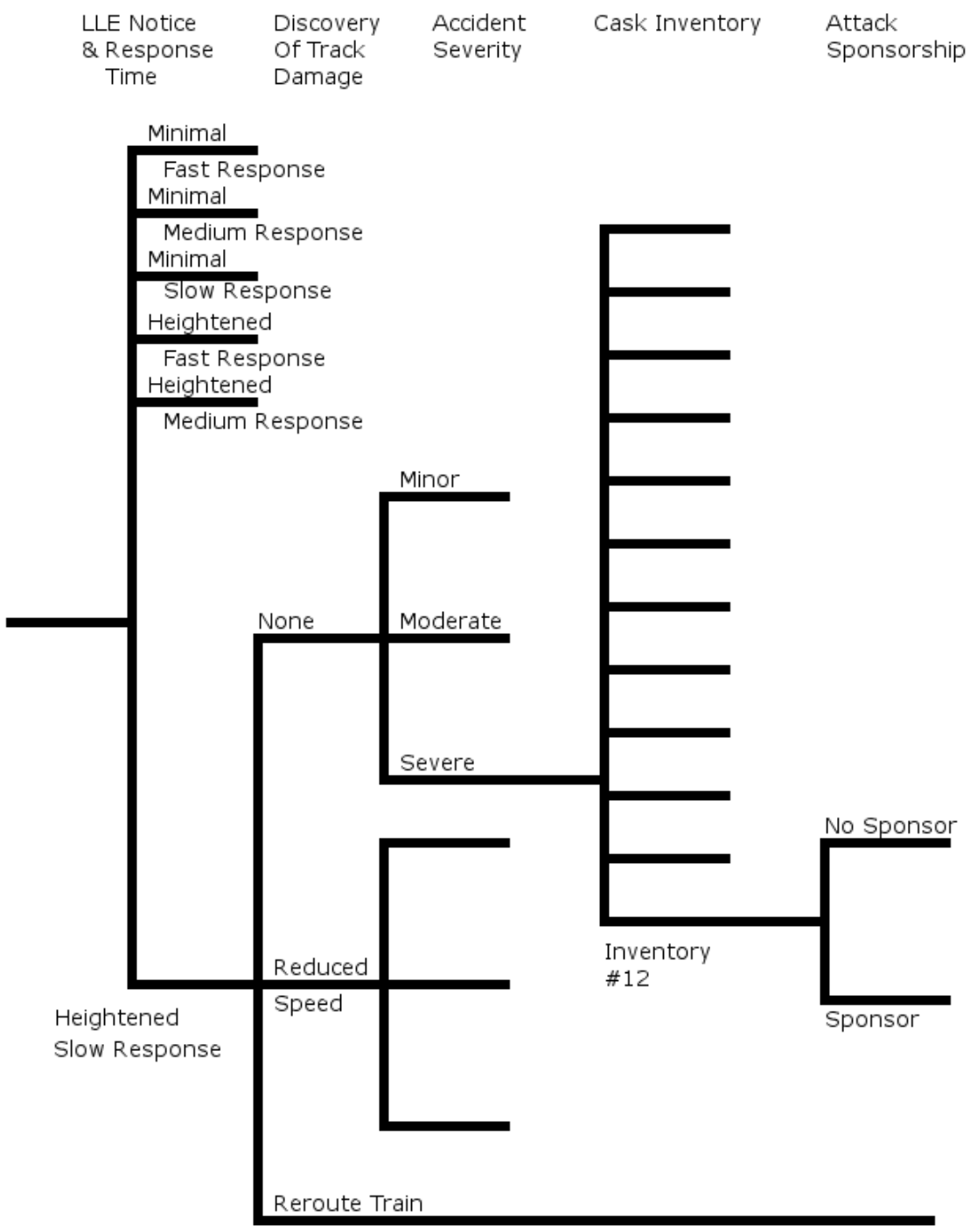


Figure 6-2 DET excerpt for Case Study 1

A subset of the total DET, consisting of 96 simulation runs were considered in this analysis; 72 with no additional adversary delay due to wreckage and 24 with a time penalty of 40 seconds; and, each run consisted of eight adversaries, eight responders and three additional offsite responders. For each simulation run, the time of arrival for offsite responders was determined randomly. As is the case for the full scenario, the adversaries win by either breaching the cask or neutralizing all of the response forces, while the response forces win by neutralizing the adversaries before they can breach the cask. Table 6-3 shows $P_N$ for no time penalty and a time penalty of 40 seconds.

Table 6-3 $P_N$ given time penalties for adversaries resulting from wreckage around the train

| $P_N$ | |
|---|---|
| 0s Penalty | 40s Penalty |
| 90.3% | 100.0% |

Notably, the time restriction on the response forces could be directly observed as having a substantial impact on $P_N$. There were seven out of 72 simulation runs in which the adversaries defeated the response force. In three of those simulation runs, the adversaries won by breaching the SNF cask before being neutralized by the offsite response forces (who did not arrive in a timely manner). In four other simulation runs, the adversaries were able to breach the cask and neutralize the offsite response forces. Furthermore, the time margin in response victories was sometimes worryingly small, with several simulation runs showing the adversaries being neutralized within 10 seconds of breaching the SNF cask—and a simulation run illustrating that the final adversary was only defeated 0.033 seconds before the adversaries would have successfully breached the

cask. When the adversaries were assessed a time penalty, there was never a concern about the cask being breached before the end of the engagement. The last adversary was neutralized, on average, about a minute before the cask would have been breached.

An additional challenge that the response forces had during Case Study 1 was that the onsite and offsite forces were unable to coordinate their response tactics. The time pressure, combined with the lack of knowledge about when the other response force would arrive and deploy, lead to the response forces engaging in a piecemeal fashion, with reduced effectiveness. This also was true for the case in which there was an imposed time penalty but given the increased time the response forces had available, some amount of coordination between onsite and offsite forces could be achieved.

For this analysis, it is possible to add on additional codes or branches based on user desire. For example, a safeguards model can be integrated into this analysis by adding an additional branch that considers the success or failure of the adversaries to breach the cask. If the cask is not breached, the analysis would terminate at the end of Phase 2. Instead, if the adversaries succeed in breaching the SNF cask, the analysis could be extended into a Phase 3 to model the safeguards risks, where branching rules based on different estimations of radioactive release divide the scenario into different amounts of unrecoverable SNM, which are not possessed by a proliferating actor. Additionally, the scenario can branch based on the expected time necessary to return the damaged SNF cask to a viable inspection site, which can itself be modified based on the amount of damage to the SNF.

These insights suggest that DPRA:

1. can be used to model and quantify how different safety and security metrics interact to result in undesired system behaviors, and;
2. offers a novel analytical technique capable of evolving and growing with real-world event complexity.

Taken together, this meta-analysis argues that DPRA can be extended to better address the growing risk complexity that 21st century environments pose to international SNF transportation (and likely other nuclear fuel cycle activities).

## 6.2 LS/TS Framework

Based on the experience of Case Study 1, some challenges were discovered in using the existing ADAPT multi-simulator framework to accommodate 2S analyses. As the existing structure requires the analyst to select which simulator is next run at every BC, the analyst is required to have advanced knowledge of which simulator would next reach a BC. Additionally, ADAPT only runs one simulator for each branch. When running safety and security simulations with explicit time parameters, it may be advantageous to run both simulations simultaneously to reduce the need to have one simulation 'go back in time' and risk that simulation's results invalidating analysis that was already performed by another simulation. For example, if at a given time $t$ a branching occurs in safety code, the next BC of the safety code might occur at $t + 10h$, but there might be a BC which would occur in the security code at time $t + 40m$. As BCs within either the safety or security models can have implications which affect both models, the branch that occurred in the security code at time $t + 40m$ may affect how the

safety code runs past time $t + 40m$. If the safety code runs with the conditions at t until time $t + 10h$ without taking into account the branching of the security code at time $t + 40m$, many hours of computing time may be spent on the safety code analyzing an inaccurate condition (i.e., nonfunctional state) of the plant. Beyond the computational time that was spent analyzing a nonfunctional state, it may not be possible to recover the plant status; typically plant safety models are only saved when branching occurs to reduce unnecessary bloat in file sizes.

Due to the limitations of the current ADAPT multi-simulator structure, it would be difficult to perform a 2S analysis where both safety and security are fully integrated. Therefore, the 2S analysis will, instead of using ADAPT's current multiple simulator functionality, manually implement a method of branching adapted from the ADS-IDAC philosophy, introduced in Section 5.3.5.

If either ADS or IDAC reach a BC, the other model receives that information immediately and can incorporate the necessary changes. The downside of the ADS-IDAC philosophy is that in order to transfer data between both models at each time step, it is a practical necessity for both models to be connected through memory, rather than exiting and transferring files. Because the models do not fully close when transferring between simulators or when undergoing branching, the simulation cannot be resumed if one branch were to fail, and the data generated up to that point would be lost. The necessity of transferring information through memory rather than through files also requires more effort developing the linkages between the simulators of choice, which increases the

difficulty for users following this methodology creating links between their codes of choice.

Because the additional time needed to transfer files makes changing simulators at each time step impractical, the methodology used in this dissertation makes use of a hybrid system combining the ADS-IDAC approach and the ADAPT approach. This hybrid system uses short time blocks of lengths which can be customized by the analyst. In this hybrid system, one model is designated as the Leading Simulator (LS). The other model is designated the Trailing Simulator (TS). The LS/TS methodology is illustrated in Figure 6-3. Each ADAPT-generated branch begins with execution of the LS, which operates until either it reaches a BC or the end of the current time block. During this simulation, the state of the LS can be saved at regular intervals. After the LS completes, the TS operates until either reaching a BC or the time block ends.

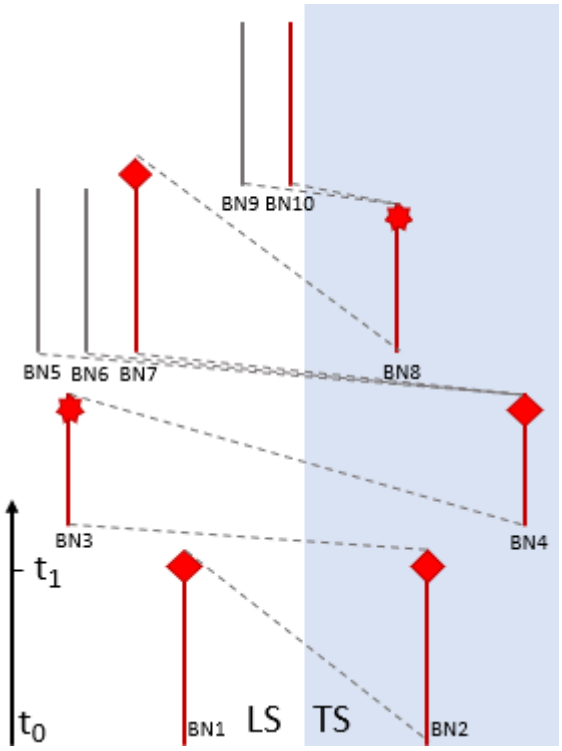


Figure 6-3 Example LS/TS structure (Diamond heads represent time blocks with no BC and starburst heads represent a BC occurring). BN: Branch Number

If the TS completes its simulation time without reaching a BC, the LS will restart and all previous restart files will be deleted from the save memory. However, if the TS reached a BC during this time, the LS will be resumed from the nearest saved state to the simulation time the TS branching. In Figure 6-3, the scenario begins at time *t*=0 with the LS Branch Number (BN) 1. This simulation continues for a fixed time block before ending at $t = t_i$ without any BCs being met, which is represented by the diamond shape terminating the simulation. The TS in BN2 is then called at time $t = 0$ to determine if this simulator reached any BCs before $t_i$. The diamond end cap shows that BN2 TS did not and the LS is restarted at time $t_i$ with BN3. Sometime before the end of this time

block the LS reached a BC, marked by the star end cap. BN4 was then called at time $t_1$ to determine if it would reach a BC before the time the LS did. As the BN4 TS did not, the LS BCs are called which leads to BN5, BN6 and BN7, beginning at the time the LS reached the BC. Following just BN7, the LS did not reach a BC in the next time block, and BN8 was again restarted from the beginning time of the most recent LS run. In this case, however, the TS has reached a BC during the time block, as marked by a star end cap. BN8 has two child branches (BN9 and BN10) which were restarted from the LS at the time of the BC by the TS. Under the LS/TS framework, new branches will always be explored first by the LS and the TS will only play catch-up, never extending its simulation time beyond that of the LS.

The LS/TS methodology automates a number of potential conflicts between simulators. Due to the nature of the time blocks used in the LS/TS method, the TS cannot continue its simulation beyond the LS. Therefore, if both the LS and the TS reach a BC during the same time block, the BC from the TS occurs before the BC from the LS, which provides a consistent method to evaluate BCs and pass information between simulators. In addition, the LS/TS methodology can be extended to an arbitrary number of simulators by adding additional TSs (such as $TS_1$, $TS_2$ and so forth). Adding further TSs does not change the structure of the LS/TS methodology.

## 6.3 Case Study 2: Scribe3D LS/TS Test Scenario

A simple test scenario was developed to serve as a case study for the proposed LS/TS methodology. For this test scenario, instances of Scribe3D are used for the LS/TS method. One Scribe3D instance models an adversary and the other models a responder

within the hypothetical Lone Pine Nuclear Power Plant (LPNPP). By using two instances of Scribe3D as the LS and TS, which can be recreated as a single Scribe3D model, the ability of the proposed methodology to create an integrated analysis is tested and any errors introduced by the methodology can be identified. For Case Study 2, the adversary attempts to sabotage an NPP or neutralize the guard force without being defeated. The potential adversary targets are the following

- The control room (CR);
- An emergency diesel generator (EDG), or;
- The CAS.

In order to accomplish their mission, the adversary must perform the tasks in Table 6-4.

In the event of an adversary attack, the responders also have a set of tasks to perform to protect the plant, given in Table 6-5. Notably, the responders are unable to begin performing their tasks until the adversary has been detected and assessed on the NPP grounds. This is assumed to occur when the adversary crosses the PIDAS, which normally includes a sensor suite for this purpose. As the responders do not know what the adversary target is, they are required to perform each of these tasks regardless of the true adversary target.

Table 6-4 Adversary tasks with associated completion times. Tasks that require negligible time or with derived completion times from the Scribe3D simulation are indicated with task times of "-".

| Task Number | Adversary Task | Time to perform |
|---|---|---|
| 1 | Breach outer PIDAS fence | 10s |
| 2 | Cross PIDAS | - |
| 3 | Breach inner PIDAS fence | 10s |
| 4 | Cross yard to NPP | - |
| 5a | Cross NPP to CR | - |
| 6a | Destroy CR systems | 15s |
| 5b | Enter EDG building | - |
| 6b | Destroy EDG | 20s |
| 5c | Cross NPP into CAS | - |
| 6c | Enter CAS | - |
| 7c | Neutralize guard | 1s |

Table 6-5 Responder tasks with associated completion times. Tasks that require negligible time or with derived completion times from the Scribe3D simulation are indicated with task times of "-". *Note that responder actions begin at the time of adversary detection and assessment*

| Task Number | Response Force Action | Time to perform |
|---|---|---|
| 1 | Receive alarm | - |
| 2 | Gear up | 20-40s |
| 3 | Move to CR | - |
| 4 | Clear CR of adversaries | 2s |
| 5 | Move to EDG building | - |
| 6 | Clear EDG of adversaries | 2s |

For simplicity, it is assumed that if the responder reaches a target before the adversary has sabotaged it, the adversary is neutralized. Additionally, if the adversary attempts to neutralize the responder before they have completed gearing up, the adversary will be successful. However, if the guard force finished gearing up before the adversary attempts to neutralize them, the adversary is defeated. An overlay of adversary and responder movements throughout LPNPP is given in Figure 6-4. The adversary and its pathway are marked in red, while the responder and its pathway are marked in blue. The EDG is to the top of Figure 6-4. The CAS contains the responder and the CR is to the bottom of Figure 6-4.

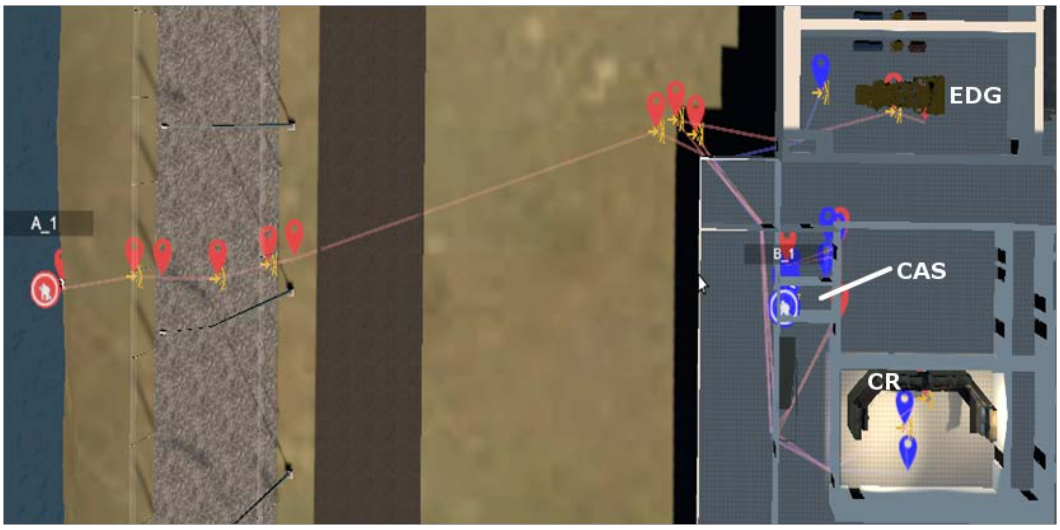


Figure 6-4 Adversary and responder pathways

For the LS/TS methodology, the analysis was split into two separate Scribe3D simulations, one modeling the adversary $A_1$, and a second which models the responder member $B_1$. Neither Scribe3D simulation contained any information pertaining to the other force. The adversary was arbitrarily chosen to be the LS and a time-block of $\Delta t = 10s$ was selected.

For this scenario, the BC occurs on the detection of the adversary while crossing the PIDAS, Task 2 in Table 6-4. When this occurs, the response tasks in Table 6-5 begin with Task 1 and the responder begins their preparations. Three child branches are created in the DET to represent uncertainty in the preparation time, one with preparation time of 20s, one with 30s and one with 40s. The second BC is when the adversary reaches the NPP structure. At this BC, the adversary determines their target. While this uncertainty does not have a probability that can be associated with it, the DET structure can inform analysts of the effects of this adversary decision and the effects it would have. The combined operator and responder tasks, and the uncertainties associated with the scenario, are given in Table 6-6.

Table 6-6 Combined adversary and response tasks, with uncertainties identified

| Adversary Task Number | Adversary Task | Adversary Task Time | BC | Responder Task Number | Responder Task | Responder Task time |
|---|---|---|---|---|---|---|
| 1 | Breach outer PIDAS fence | 10s | - | | | |
| 2 | Cross PIDAS | - | Select gear up time | 1 | Receive alarm | - |
| 3 | Breach inner PIDAS fence | 10s | - | 2 | Gear up | [20s, 30s, 40s] |
| 4 | Cross yard to NPP | - | Select adversary target (a, b, or c) | 3 | Move to CR | - |
| 5a | Cross NPP to CR | - | - | 4 | Clear CR of adversaries | 2s |
| 6a | Destroy CR systems | 15s | - | 5 | Move to EDG building | - |
| 5b | Enter EDG building | - | - | 6 | Clear EDG of adversaries | 2s |
| 6b | Destroy EDG | 20s | - | | | |
| 5c | Cross NPP into CAS | - | - | | | |
| 6c | Enter CAS | - | - | | | |
| 7c | Neutralize guard | 1s | - | | | |

Section 6.3.1 describes the effects of the adversary targeting the control room, Section 6.3.2 describes the effects of targeting the CAS and responder, and Section 6.3.3 describes the adversary targeting the EDG. Section 6.3.4 compares the results of the LS/TS method to the results obtained by modeling the scenario in one Scribe3D simulation.

### 6.3.1 Control Room (CR)

The adversary attack on the CR requires the adversary to enter the NPP structure and pass close to the CAS to arrive at their target. The responder, after completing their preparation, additionally travels directly to the CR. The times of the scenario completion and winning entity are given in Table 6-7.

Table 6-7 Results of CR sabotage

| Preparation Time | End time (s) | Winning Side |
|---|---|---|
| 20s | 47.5 | Responder |
| 30s | 57.6 | Responder |
| 40s | 64.8 | Adversary |

As there are no modeled uncertainties in the adversary timeline, their time of task completion remained unchanged. However, as the responder had uncertainty in their preparation time, their time of arrival within the CR was uncertain. Additionally, the overall simulation was terminated on either side reaching their success criteria, which resulted in the end times initially occurring due to the responder arrival. Once the preparation time increased, the adversary completed its task without interruption, leading to the fixed scenario end times.

### 6.3.2 Central Alarm Station (CAS)

When the CAS is the adversary target, it is assumed that to be successful the adversary must defeat the responder. For this subcase the simulation was evaluated until the adversary reached the CAS, regardless of when the responder completed their

preparations. As there is no uncertainty in the adversary timeline, this simulation always ends at 52.1 seconds. Results are summarized in Table 6-8.

Table 6-8 Results of CAS sabotage

| Preparation Time | Winning Side |
|---|---|
| 20s | Responder |
| 30s | Responder |
| 40s | Adversary |

For both 20s and 30s of preparation times, the responder defeats the adversary by completing preparations before the arrival of the adversary. The adversary only wins when the responder requires 40s of preparation time. Since the time the responder completes their preparations was not chosen as a stopping condition, the exact times that this occurred were not included in Table 6-8.

The results of these DET branches were investigated to determine the time that the responder completed their preparations. This was done by rerunning the last time-block in the responder simulation before the responder was fully prepared. Using results from the DET, rather than performing a new analysis, allows the simulation to incorporate the detection time from the DET as well as the uncertainty in the time to complete the gear up task. For 20s preparation time, the responder completed this task at 36.5 seconds, for 30s preparation finished at 46.5 seconds and for 40s preparation time the adversary neutralized the responder at 52.1 seconds.

### 6.3.3 Emergency Diesel Generator (EDG)

For this adversary target in the LPNPP, reaching the EDG does not require the adversary to enter the main plant structure and instead has access through an external door, following the path shown in Figure 6-4. Despite the task of destroying the EDG

having a longer task time than sabotaging the CR, here the adversary is successful for a 30s responder preparation time. The results are summarized in Table 6-9.

Table 6-9 Results of EDG sabotage

| Preparation Time | End time (s) | Winning Side |
|---|---|---|
| 20s | 61.6 | Responder |
| 30s | 63.8 | Adversary |
| 40s | 63.8 | Adversary |

### 6.3.4 Comparison with Direct Solution

By creating a joint scenario in Scribe3D that models both the adversary and the responder, each of the scenarios investigated using the LS/TS method can be compared to a direct evaluation of the timelines, using Scribe3D to simulate each of the DET sequences without using the LS/TS approach. The purpose of this comparison is to identify any errors introduced to the scenario through the LS/TS methodology. The results of this direct comparison are summarized in Table 6-10.

The cause of the difference in the end times of the LS/TS method compared to the direct solution appears to be related to the simulation process of Scribe3D. As Scribe3D uses time steps of finite length for its simulation process, these introduce minor errors in the necessary time to complete tasks. However, the magnitude of these errors is negligible and a necessary consequence of performing many simulations and is not restricted to Scribe3D or the LS/TS method.

Table 6-10 Comparison between LS/TS and directly calculated results

| Preparation Time | Target | Differential End Time | Change in Outcome |
|---|---|---|---|
| 20s | CR | -0.1 s | No Change |
| | CAS | 0.2 s | No Change |
| | EDG | 0.1 s | No Change |
| 30s | CR | -0.1 s | No Change |
| | CAS | 0.1 s | No Change |
| | EDG | 0 s | No Change |
| 40s | CR | -0.4 s | No Change |
| | CAS | 0.1 s | No Change |
| | EDG | 0 s | No Change |

The results in Table 6-10 demonstrate that the LS/TS methodology coupled with ADAPT successfully links multiple simulators together and reproduces results obtained from a single simulator. The LS/TS methodology ensures that the simulators progress through the scenario in a quasi-simultaneous fashion, which ensures that the BCs occur in the correct order and at the same time for all included simulators. The use of ADAPT branching rules ensures that information is transferred between the simulators as necessary. As there are no simulators that model both NPP security and safety procedures, Case Study 2 results illustrate that the LS/TS approach can link multiple simulators necessary to perform DET analysis of a 2S system.

# Chapter 7 - Case Study 3: Integrated Safety-Security Analysis for LPNPP

In this chapter, a case study involving the LS/TS methodology introduced in Section 6.2 is performed. This case study explores a successful adversary attack on the hypothetical LPNPP using two computer models:

- Scribe3D (Section 5.1.3) serving as a FoF model, and;
- MELCOR, (Section 5.2.1) a reactor response model.

These models are integrated into a single DPRA process using the LS/TS methodology and the ADAPT branching strategy which examines operator and plant response alongside FoF analysis. In this case study, Scribe3D is used to determine the timing and extent of sabotage and repair actions by explicitly dispatching adversary and operator entities to locations around LPNPP and performing the necessary tasks. The MELCOR code determines the effects of these actions performed by Scribe3D entities on the reactor and calculates the time it becomes necessary for operators to initiate repair actions. The combined analysis is then analyzed to determine the effects of the security system on the reactor response and to demonstrate the effects of safety systems after sabotage as sabotage mitigation. The ADAPT wrapper file for Case Study 3 is shown in Appendix C.

LPNPP was first created in 2011 as a hypothetical PWR for training on nuclear security and VAI. This initial incarnation of the LPNPP included exterior plant layouts but was not modeled for detailed safety analysis and did not have interior layouts modeled. A rendering of the original facility is shown in Figure 7-1.

Figure 7-1 Original LPNPP rendering [76]

In later years, this model was further refined and modified, which involved changing the site layout, adding interior details, and building the model in several of the computerized FoF codes introduced in Section 5.1, including Simajin and AVERT. In 2016, LPNPP was integrated into the 26$^{th}$ International Training Course (ITC). The ITC is a 3-week IAEA course to train global participants on physical security, and teaches the DEPO method outlined in Chapter 3. To support the use of the LPNPP within the ITC, the model was again refined and further updated to include a full internal and external layout.

In 2019, the SSCs in LPNPP were updated to more accurately reflect, including replacing the initial reactor coolant system with one based on the Three Mile Island Unit 2 reactor. Additionally: i) the turbine building was upgraded to add additional detail and a

FLEX building was added to the LPNPP site, and, ii) a previously existing MELCOR model of the Three Mile Island Unit 2 reactor was adapted into a LPNPP model to perform a station blackout analysis of the system response. These efforts are detailed in [76].

Section 7.1 describes LPNPP's layout and vital areas, Section 7.2 describes the scenario and its implementation, Section 7.3 covers the branching parameters used in this study and the results are shown in Section 7.4. The conclusions reached in this case study are summarized in Section 7.5.

## 7.1 LPNPP Description

The LPNPP hypothetical NPP was built in 1972 to produce 1150 megawatts electrical for the Republic of Lagassi power grid. The plant is located on the north shore of Lake Winowich. The LPNPP is a PWR with a closed primary coolant loop which is connected to a secondary power conversion system which carries steam to the turbine. A generic example of a PWR is given in Figure 7-2. The coolant used in the primary system is light water under high pressure, typically around 2235 psi. In addition to light water, the primary coolant includes boric acid to control the reactivity and other chemicals to reduce corrosion. The steam from the secondary coolant travels to the turbines where much of the thermal energy is converted into electrical energy, before rejecting the remaining heat to the condenser and returning to the steam generators via feedwater pumps.

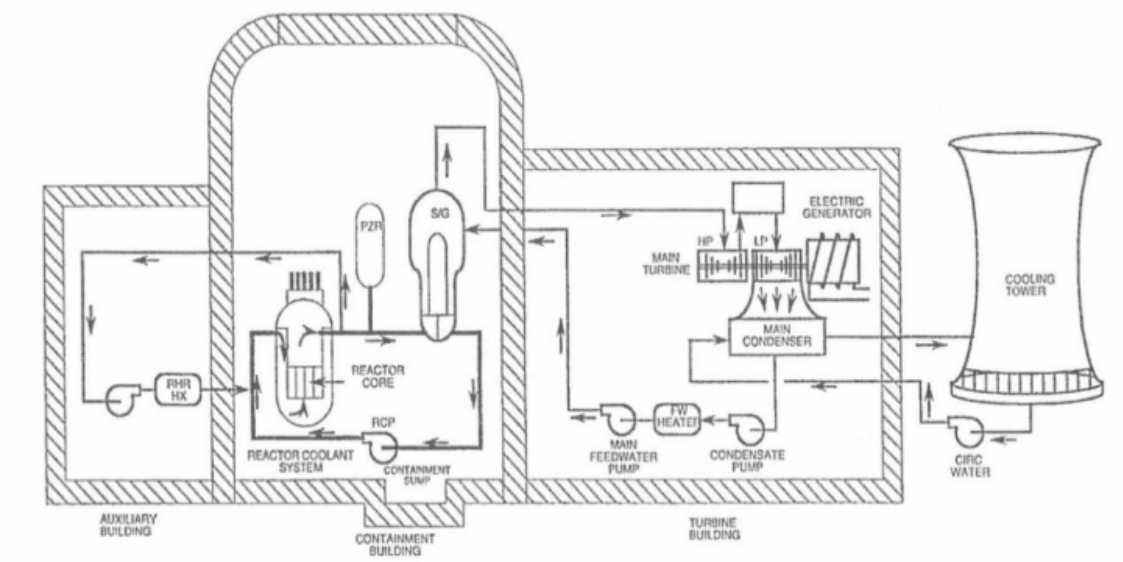


Figure 7-2 Generic PWR arrangement

The layout of LPNPP is shown in Figure 7-3. This layout includes all major buildings within the site area and shows the locations of guard posts and patrols. The intake building is to the south of the site, bordering Lake Winowich. The FLEX building is an orange-marked standalone structure to the north of the CAS. The double-fence of the PIDAS is shown surrounding the LPNPP buildings, which also contains the guard towers.


Figure 7-3 Layout of the LPNPP site

Vital areas of LPNPP are rooms within the plant that are used to ensure cooling of decay heat from the reactor fuel and spent fuel. These areas are originally created as candidate vital area sets, each of which is one of the different combinations of rooms which contain sufficient systems to provide a single train of cooling capability to the reactor fuel. One of these candidate vital area sets is then selected to be protected as the vital area set.

Some vital areas are uniquely necessary, such as the containment structure, and must always be protected to prevent radiological sabotage. Other vital areas, such as specific battery rooms, are selected to ensure one safety train remains operational. However, because protecting all vital areas is sufficient to prevent sabotage, regardless of which of many sabotage scenarios adversaries might wish to undertake, it is necessary for the physical protection system to prevent access by adversaries to any of the vital areas. One vital area set, with the minimum number of protected rooms, is in Table 7-1. Note that due to the nature of LPNPP as a hypothetical reactor used for security analysis, several of the vital area locations are not fully defined. Figure 7-4 and Figure 7-5 show the Scribe3D model of LPNPP with important locations for this case study marked.

Table 7-1 LPNPP Vital Areas

| Vital Area | Area Location |
|---|---|
| Auxiliary Feedwater (AFW) Turbine Driven Pump Room | Engineered Safety Building |
| Battery Room A | Control Building |
| Cable Spreading Room | Control Building |
| Reactor Containment | Containment Building |
| Main Control Room | Control Building |
| Condensate Storage Tank | Site Protected Area |
| Condensate Storage Tank Piping | Site Protected Area |
| Spent Fuel Pool | Fuel Building |
| Main Steam Valve Building | Site Protected Area |
| Scram Relay Room | Control Building |

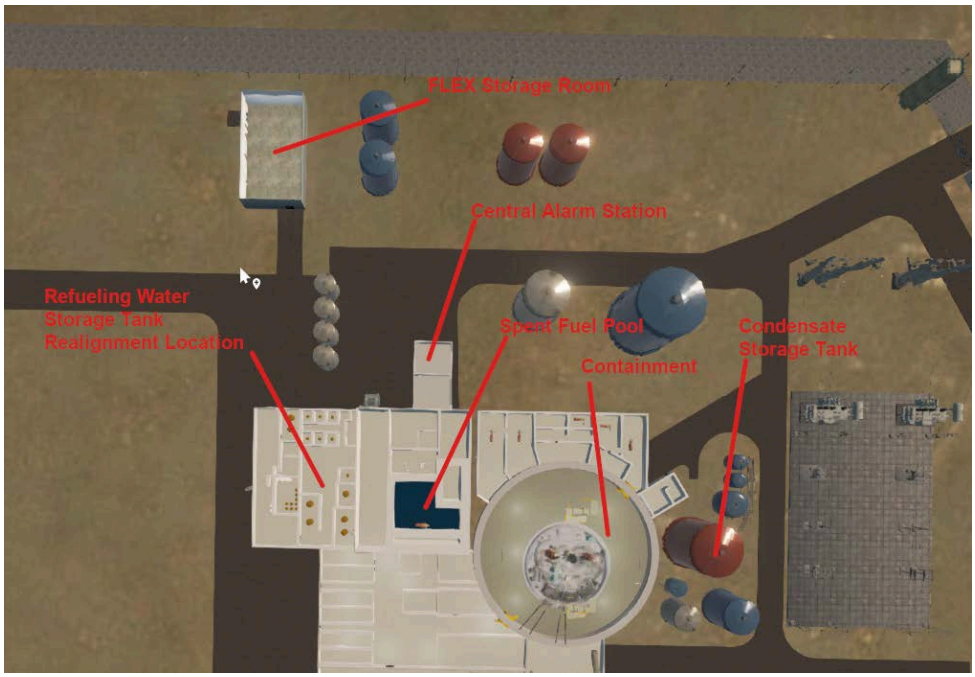


Figure 7-4 Scribe3D model of LPNPP – North End

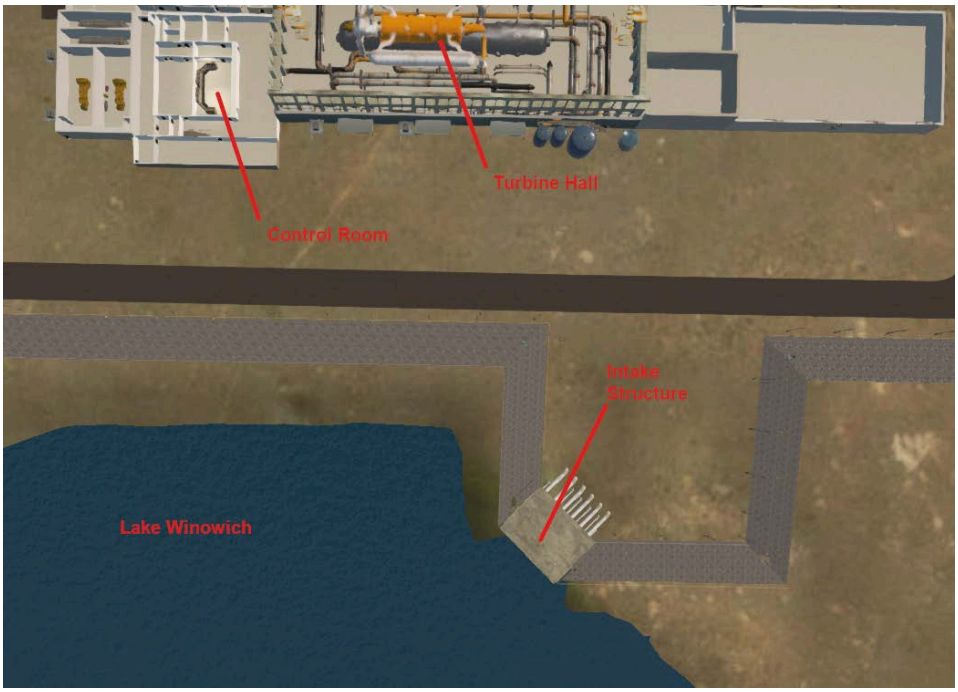


Figure 7-5 Scribe3D Model of LPNPP – South End

## 7.2 Scenario Description

In 2011, a VAI of the LPNPP model, as it existed at the time, was performed. This VAI was used to determine the locations or combinations of locations that, if sabotaged by adversaries, would result in radiological release. This process required characterizing the SSCs within the LPNPP and associated dependencies to generate the necessary FT, an example of which is given in Figure 7-6.

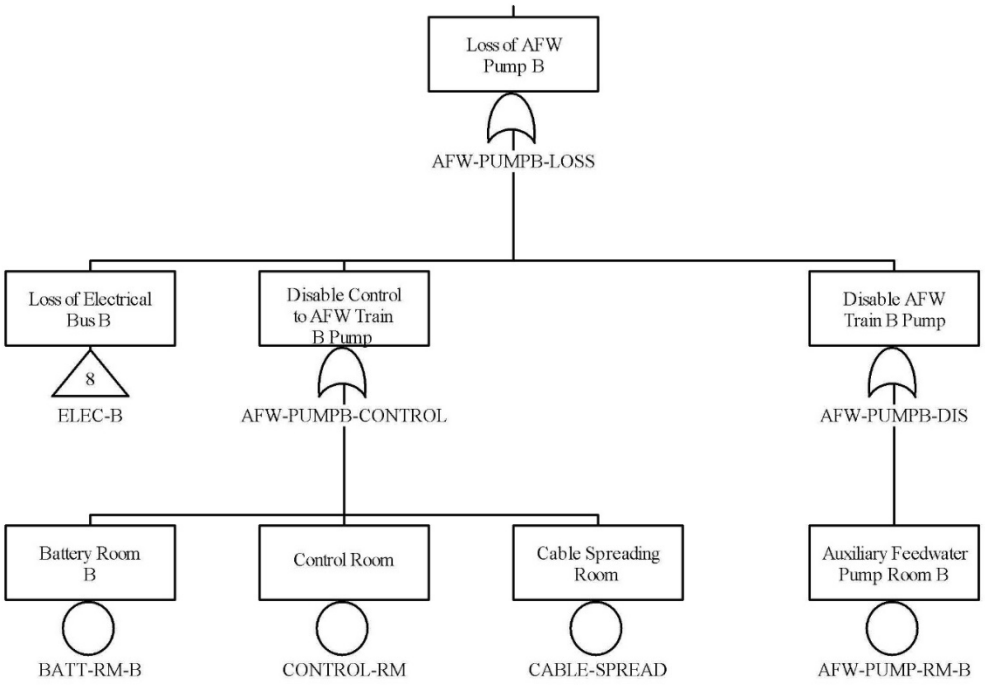


Figure 7-6 Selection of sabotage area logic model developed for LPNPP

However, due to the updates and changes to systems within the LPNPP since this VAI's construction, some of the vital areas found by this analysis may no longer hold. Therefore, a scenario was chosen which relies on systems that were unchanged during the updates to the LPNPP. The chosen scenario is a loss of ultimate heat sink, which has the

intake structure and the CST as the target set. However, FLEX was not instituted in plants at the time of the VAI, and as FLEX is intended to have all necessary equipment to maintain core integrity, the FLEX building was additionally considered a potential adversary sabotage target.

A scenario involving an attack on this expanded target set was constructed for Case Study 3. This scenario involves an adversary force consisting solely of outsiders that was divided into two teams. Team RED 1 consists of marksmen armed with long range rifles emplaced within line of sight of the LPNPP. Team RED 2 begins on the shore of Lake Winowich, having disembarked from a boat used to approach LPNPP. At the beginning of the scenario, RED 1 neutralizes the guard towers while RED 2 crosses the PIDAS and enters the intake structure. Once inside the intake structure, RED 2 sabotages the pumping equipment supplying water to LPNPP.

After sabotaging the pumping equipment, RED 2 leaves the intake structure and crosses the protected area to the CST under the protective cover of RED 1. RED 2 engages and defeats the response force with the assistance of RED 1, if necessary.

Upon arriving at the CST, RED 2 creates a hole in the side of the tank in order to release the stored water. Then, if at least 3 members of RED 2 are still active, RED 2 proceeds to the FLEX building and sabotages the stored equipment. In either case, RED 2 then enters the LPNPP auxiliary building and interdicts operators attempting to travel throughout the facility while RED 1 attempts to interdict similar activities outside the facility building. When offsite responders arrive at the facility, RED 1 notifies RED 2 and

all adversaries exfiltrate LPNPP. This adversary scenario is shown in Figure 7-7, with RED 1 marked by a red pentagon and RED 2's pathway marked by the red line.

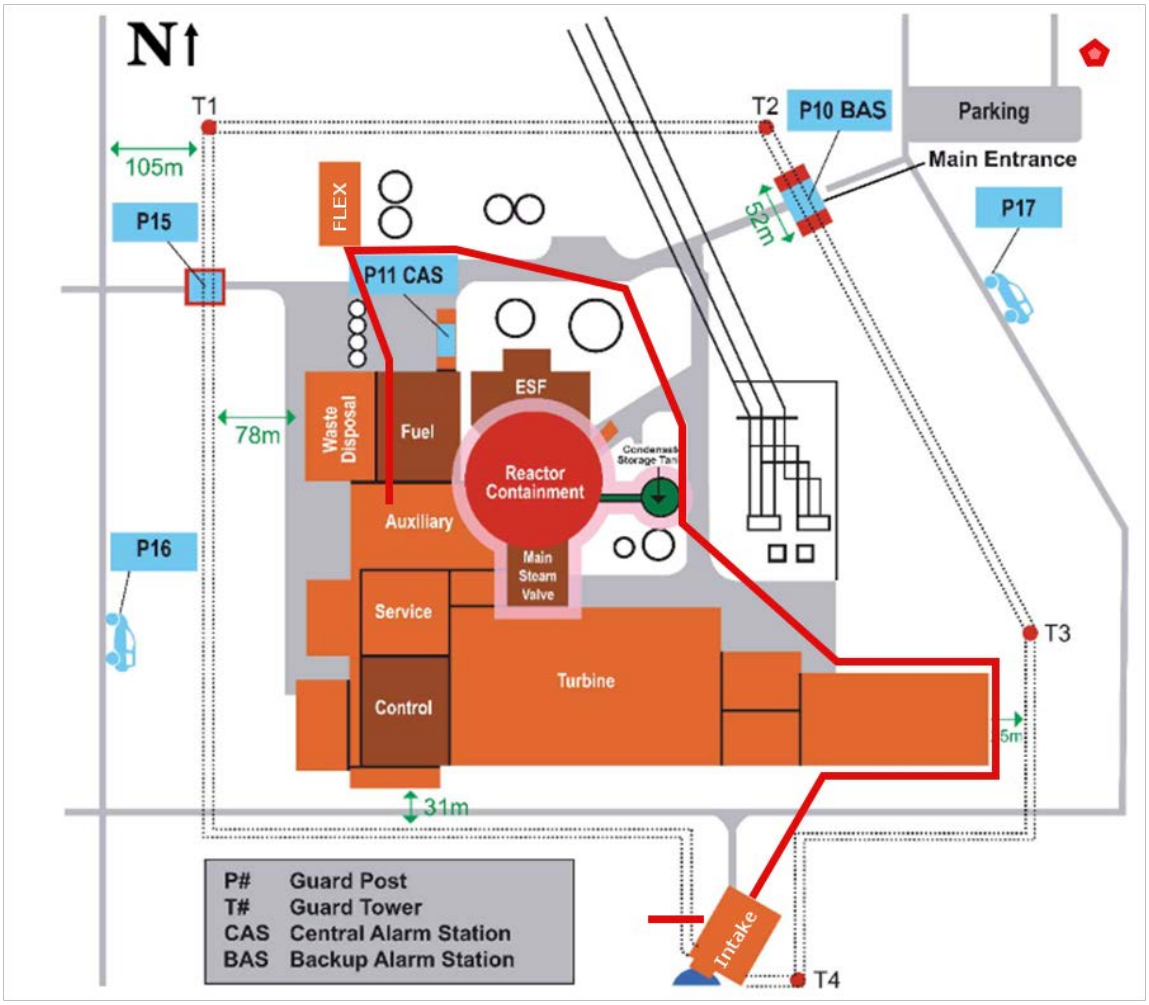


Figure 7-7 Illustration of adversary pathway through LPNPP

LPNPP initially responds to this scenario by attempting to neutralize RED 2 with response forces. If unsuccessful in doing so before the CST is damaged, the operators use the AFW system to provide secondary cooling until the CST is completely drained. Once the CST is drained, operators perform no action until the coolant temperature in the lower plenum of the reactor reaches 600K.

When the lower plenum temperature reaches 600K, the operators perform a field action to restore the AFW. As adversaries are still present in LPNPP, operators will call for a member of the security force (BLUE 1) to provide an escort. An operator then travels with BLUE 1 to the auxiliary building to align the Refueling Water Storage Tank (RWST) with the AFW system. If this operator is killed by interdicting forces from RED 2, no operator will leave the control room until offsite responders clear the facility of adversaries.

For the purposes of this case study, it is assumed that offsite responders clear the plant of adversaries and implement FLEX, if available, 8 hours after the beginning of the scenario. The modeled effect of FLEX is to supply coolant to the AFW. Finally, it is assumed that after 24 hours offsite equipment from a SAFER facility will arrive and provide cooling to the plant, so the experiment finishes at that time.

## 7.3 DET Branching Parameters

Events which occur during an adversary attack on a NPP are uncertain; the interplay between the adversaries and security operators creates a large uncertainty in the events and outcomes. In addition, the explicit time and order of events in nuclear security play a substantial role in the effectiveness of a PPS, as mentioned in Section 4.3. Therefore, many DET branching parameters used in Case Study 3 were based on possible events which could occur by adversaries and the response force.

The detection of adversaries is one of the critical elements of a PPS. Furthermore, as mentioned in Section 3.2, the PPS can either be timely or not, and one element that is uncertain is when adversaries are detected. For this case study, there are two branches

associated with the detection of adversaries; one timely and one not timely. As Case Study 3 is intended to serve as a demonstration of applying the LS/TS methodology to a 2S scenario, a limited number of branches were used for clarity. Additional branching could be performed to add additional fidelity to the timing of adversary detection. As adversaries first enter a detection zone crossing the PIDAS, the timely detection BC occurs while adversaries are in the PIDAS. The non-timely detection occurs when adversaries have sabotaged the intake structure and the CST.

There are two effects which occur on the detection of adversaries. The first is that the response force receives a notification of the alarm and begins their preparations to neutralize the adversaries. The second is that the reactor operators trip the reactor when notified about adversaries entering the site.

In addition to the detection of adversaries, neutralization of adversaries by the response force is a major uncertainty. While the response force at LPNPP is intended to defeat the adversaries, this outcome is not modeled, as the case where adversaries fail to complete their sabotage mission is a trivial one. Instead, the modeled branches are one where the adversary handily defeats the response force and one where the adversary narrowly defeats the response force. Additional branches could be created to model the full suite of outcomes of each engagement. Only in the case where the response force is handily defeated can the adversaries additionally sabotage the FLEX equipment. Otherwise, the adversaries proceed directly to interdicting operators.

Another uncertainty is in the extent of damage from sabotage. For many components, damage results in degradation of performance rather than a complete loss. In

this case study, the sabotage of the CST by adversaries is subject to uncertainties in the extent of damage caused, with two explored branches. In the first branch, adversary sabotage causes a circular hole with diameter of $1m^2$. In the second branch adversary sabotage causes the immediate loss of the CST. Additional degradation states can be considered using the ADAPT branching methodology.

As the reactor core progresses through the sabotage-induced accident, operators may find it necessary to attempt a field action while adversaries are still present in LPNPP. Despite having an escort from the security operators, there is a chance that operators will be killed by adversaries and the field action will fail. Two branches are explored; one branch covers the field action success and the other covers the field action's failure. In this case, the limited number of branching is used to model a binary case where an action is either performed or not performed.

A summary of all the modeled DET branching parameters and their effects on both the MELCOR and SCRIBE3D simulations is given in Table 7-2:

Table 7-2 DET Branching Parameters

| BC | Child Branch | Short Name | MELCOR Effects | Scribe3D Effects |
|---|---|---|---|---|
| **Time of adversary detection** | Timely detection | T | Immediate rector scram | Mustering of responders begins immediately |
| | Non-timely detection | N | Reactor scram on CST sabotage | Mustering of responders begins on CST sabotage |
| **Adversary engagement** | Close adversary victory | C | FLEX available at 8 hours into the scenario | All responders killed, many adversaries killed, adversaries skip FLEX sabotage |
| | Overwhelming adversary victory | O | FLEX sabotaged by adversaries | All responders killed, few adversaries killed, adversaries sabotage FLEX building |
| **Damage to CST** | CST degraded | D | $1m^2$ hole in CST | N/A |
| | CST lost | L | CST unavailable | N/A |
| **Operator Realignment** | Realignment successful | S | AFW restored at time realignment completes | RED 2 killed, operator performs realignment action |
| | Realignment failed | F | AFW not restored during scenario | Operator and BLUE 1 killed |

A sequence can be uniquely identified by the order and values of branching parameters that occur during that sequence. Sequences are assigned unique identifications based on the parameters in Table 7-2. These identifications are the short name of the branch taken for each encountered uncertainty in the order that each uncertain parameter was encountered. These sequence identifications are used for further discussion of the results.

While the DET structure was used for this analysis, no consideration was given to the conditional probabilities of any of the modeled branching parameters. Conditional probabilities are standard to include in DPRA to allow analysts to gain an understanding of the total risk. However, as described in Section 4.3, determining accurate probabilities for branching parameters corresponding to adversary behaviors is a matter subject to academic controversy, and research on determining adversary probabilities is outside the scope of this research.

Human reliability was also not considered in this analysis. In nuclear safety, the importance of reliability of operator actions has resulted in a large body of research into human reliability. Issues of human error and morale have similarly been longstanding challenges in any form of combat. However, since the objective of this dissertation is to present the methodological approach and not realistic likelihoods of outcomes, neither of the models used in this analysis include human reliability. Additionally, standard practice in nuclear security is to assume that adversaries and response forces will not willingly abandon their tasks.

## 7.4 Results

The DET resulted in 31 total branches with a total of 16 unique sequences, 6 of which did not reach completion due to MELCOR crashing. The crashed branches include all sequences where the CST was lost and realignment was successful, but as these sequences only crashed after the core temperature recovered and no damage occurred, the sequences were assumed to have no core damage occur. The other 2 crashed sequences failed after a large extent of core damage occurred, and these results were characterized

based on the incomplete results. A graphical depiction of the DET is provided in Figure 7-8. The letters at each branch describe the sequence within the DET to arrive at that branch, using the short names in Table 7-2. The red letters correspond to the short name of the current BC, while the black letters are the short names of all previous BCs/ For example, the first branching point, with child branches **T** and **N**, is the time of adversary detection. Each sequence, then, is constructed from the short names corresponding to the branches that make up the sequence in order. Sequence #NDCF has Non-timely detection, a Degraded CST, a Close adversary victory, and Failed realignment action.

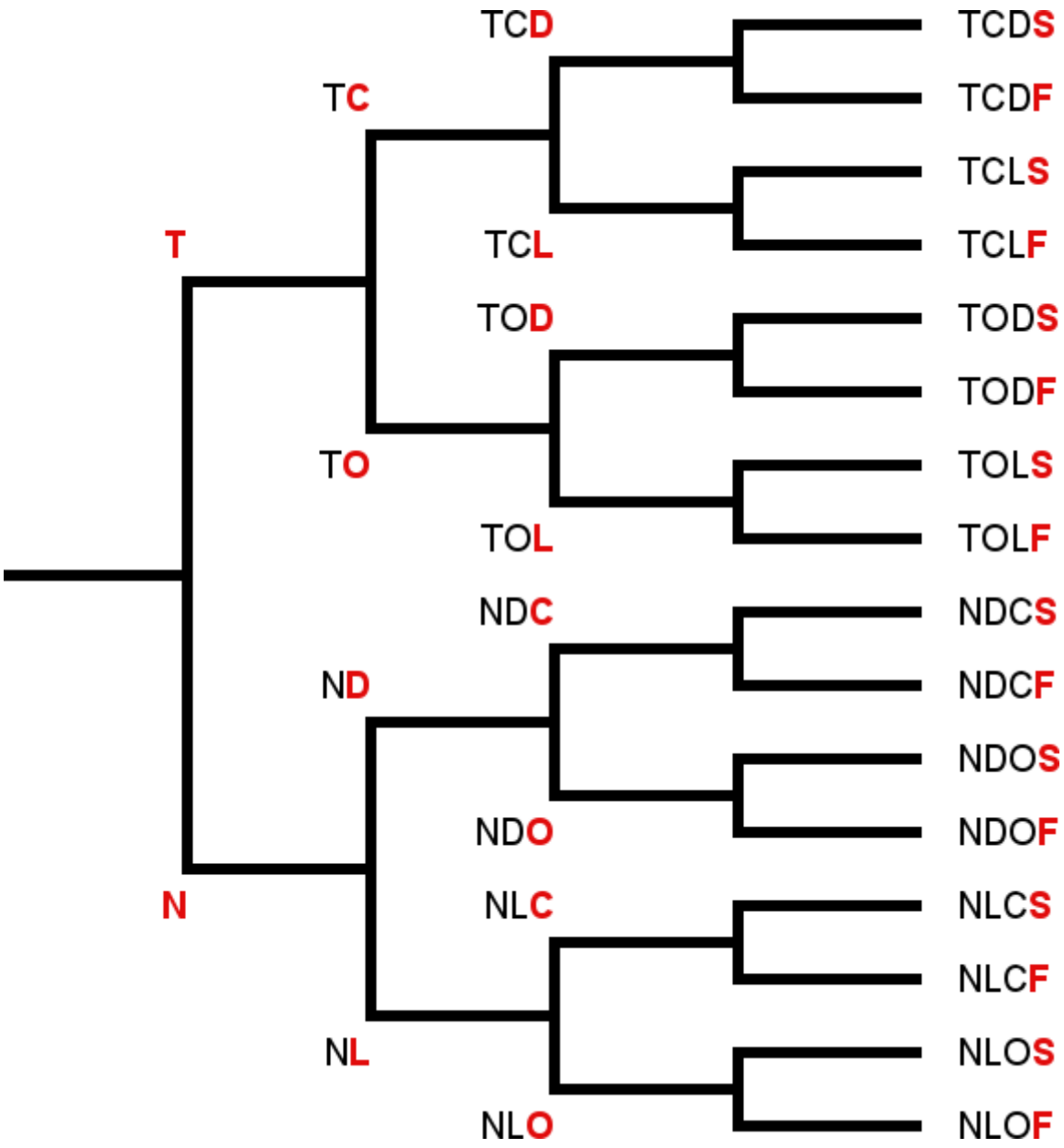


Figure 7-8 DET sequences resulting from Case Study 3 (see Table 7-2 for nomenclature)

An overview of the sequence of events is given in 7.4.1. A description of the reactor response is given in 7.4.2. Section 7.4.3 describes the integrated 2S effects, including the radionuclide release associated with this adversary attack. Section 7.4.4

provides an initial examination of the sensitivity of the LS/TS methodology to the time block length.

### 7.4.1 Scenario Timelines

One of the assumptions made for this case study is that adversaries defeat the response force and successfully sabotage the target set of the intake building and the CST. Under traditional VA, if adversaries sabotage a complete target set an unacceptable release of radionuclides is assumed to occur. In this analysis, the loss of the CST and intake structure removes all available water sources to the AFW system. The effect of this loss on the reactor, however, depends on the timing events occur at, both for events associated with security and those associated with safety. Table 7-3 outlines notable events which occur during this scenario, including both those associated with the security system and the reactor response.

Table 7-3 Times of key events for all sequences

| # | Sequence Name | Time of Detection (h) | Time of Engagement (h) | CST Sabotage Time (h) | Time of AFW Loss (h) | Time to Restore AFW (h) | Time of Core Damage (h) | Time of Radionuclide Release (h) |
|---|---|---|---|---|---|---|---|---|
| 1 | TCDS | 0.0020 | 0.0966 | 0.1206 | 2.0139 | 4.3756 | N/A | N/A |
| 2 | TCDF | 0.0020 | 0.0966 | 0.1206 | 2.0139 | 8 | 7.3334 | 7.9028 |
| 3 | TCLS | 0.0020 | 0.0966 | 0.1206 | 0.1206 | 0.8606 | N/A | N/A |
| 4 | TCLF | 0.0020 | 0.0966 | 0.1206 | 0.1206 | 8 | 2.8472 | 3.1806 |
| 5 | TODS | 0.0020 | 0.0966 | 0.1206 | 2.0139 | 4.3756 | N/A | N/A |
| 6 | TODF | 0.0020 | 0.0966 | 0.1206 | 2.0139 | N/A | 7.3334 | 7.9028 |
| 7 | TOLS | 0.0020 | 0.0966 | 0.1206 | 0.1206 | 0.8606 | N/A | N/A |
| 8 | TOLF | 0.0020 | 0.0966 | 0.1206 | 0.1206 | N/A | 2.8472 | 3.1806 |
| 9 | NDCS | 0.1209 | 0.2668 | 0.1209 | 2.0139 | 4.3533 | N/A | N/A |
| 10 | NDCF | 0.1209 | 0.2668 | 0.1209 | 2.0139 | 8 | 7.2083 | 7.7778 |
| 11 | NLCS | 0.1209 | 0.2668 | 0.1209 | 0.1209 | 1.0575 | N/A | N/A |
| 12 | NLCF | 0.1209 | 0.2668 | 0.1209 | 0.1209 | 8 | 3 | 3.3333 |
| 13 | NDOS | 0.1209 | 0.2668 | 0.1209 | 2.0139 | 4.3533 | N/A | N/A |
| 14 | NDOF | 0.1209 | 0.2668 | 0.1209 | 2.0139 | N/A | 7.2083 | 7.7778 |
| 15 | NLOS | 0.1209 | 0.2668 | 0.1209 | 0.1209 | 1.0575 | N/A | N/A |
| 16 | NLOF | 0.1209 | 0.2668 | 0.1209 | 0.1209 | N/A | 3 | 3.3333 |

From the times in Table 7-3, there are several things that can be immediately noticed. Ensuring the early detection of adversaries is a vital component of a PPS, and the detection of adversaries additionally causes the reactor to scram. Despite this scram response, failing to detect adversaries in a timely manner has a limited effect on the timing of events in the reactor (compare Rows 1 and 5 to Rows 9 and 13, or compare Rows 3 and 7 to Rows 11 and 15). Additionally, these effects are inconsistent. If the CST is lost, core damage occurs earlier in the case where reactor scrams earlier, as shown in the time of core damage column for Rows 3 and 7 compared to Rows 11 and 15. However, if the CST was only degraded, core damage occurs later for sequences where

the reactor scrams earlier. Rows 1 and 5 compared to Rows 9 and 13 illustrate this behavior.

The successful realignment of the RWST to the AFW system prevents any core damage. Table 7-3 shows the time that successful realignment occurs and the AFW system with restored, which occurs in all odd-numbered rows. In all even-numbered rows, the realignment action is unsuccessful and reactor core damage occurs. However, the other events in the sequences have an effect on the timing of reactor damage and radionuclide release.

The branching parameter that has the greatest effect on the damage time is the extent of damage to the CST. Damage to the CST rather than an immediate loss delays the time before the reactor reaches core damage by several hours. In all cases, however, core damage occurs before FLEX can restore the AFW at 8 hours into the scenario (see Table 7-3).

The average difference in time to core damage is 4.347 hours between those branches where adversaries completely destroy the CST (Rows 3, 7, 11, and 15) and those where adversaries create a hole in the CST wall (Rows 1, 5, 9, and 13). The cause of this is that damaging the CST leaves the AFW system providing coolant to the secondary system until the CST has fully drained. The CST retains enough water to supply the AFW system for 1.893 hours. This capability provides additional cooling to the reactor as the decay heat produced by the reactor drops over the time period where the AFW system is functioning.

### 7.4.2 Reactor Response

The core inlet temperature for all sequences can be seen in Figure 7-9. Sequences where the CST was lost are shown in blue, and those where the CST was degraded are shown in red. The loss of available AFW prevents the plant from supplying additional coolant to the steam generators, causing a rise in temperature to above 600K. For the cases where the CST was lost, this rise in temperature can be seen occurring at the beginning of the scenario. For the cases where the CST was degraded, this rise in temperature due to AFW unavailability begins 3 hours into the scenario. For the first 2 hours of this scenario, while the AFW system functions, the core temperature instead drops. Once all cases reach a temperature of slightly over 600K, the temperature remains constant for 3 or 4 hours, depending on the sequence without mitigation. The primary coolant is at the saturation temperature and is boiling during this period. The core dryout in these unmitigated cases are marked by sudden spikes in the core temperature, which soon rises to over 1000K as the accident sequence progresses. For cases where the CST is lost, this rise in core temperature (approximately 4 hours into the scenario if the CST is lost and 9 hours into the scenario if the CST is degraded) associated with dryout can be seen occurring approximately 4 hours into the scenario, while this occurs approximately 9 hours into the scenario if the CST was degraded.

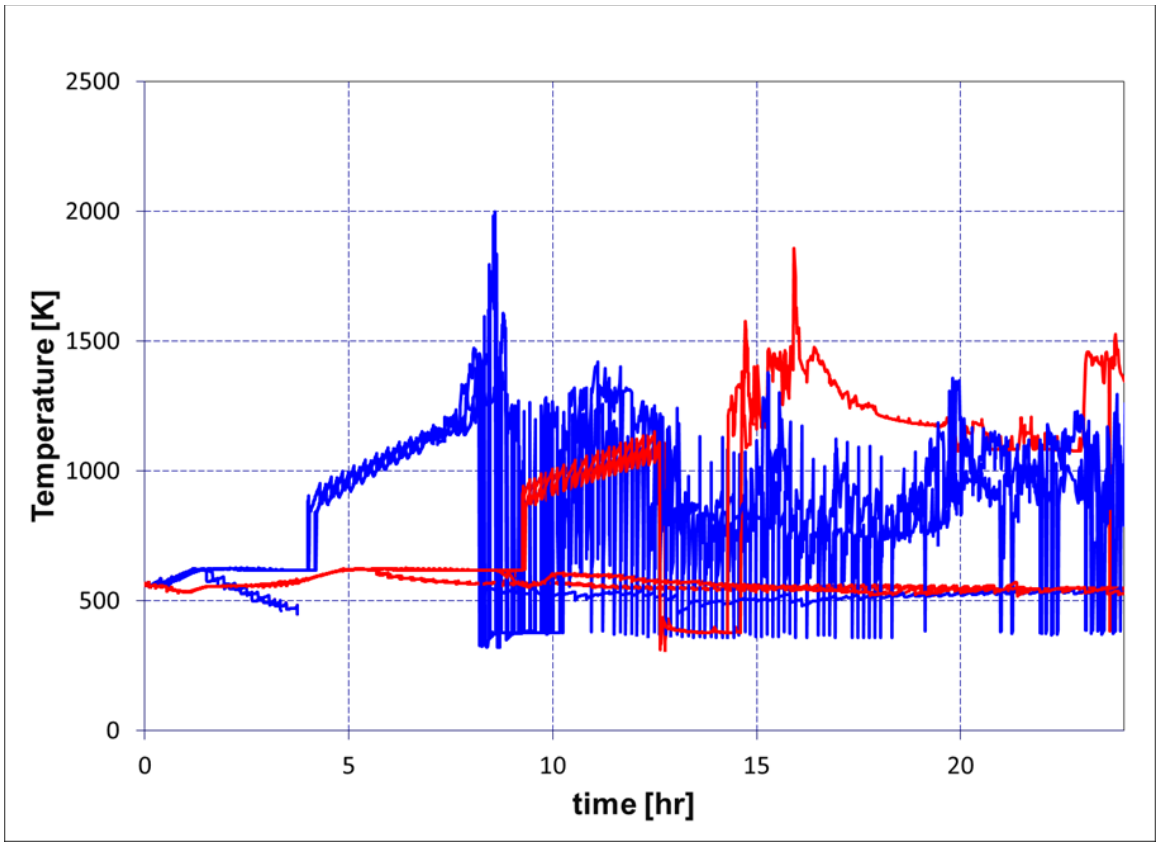


Figure 7-9 All observed core inlet temperatures during Case Study 3. Note that sequences where the CST was lost are shown in blue, and those where the CST was degraded are shown in red

In Figure 7-9, divergence in the temperature plots occurs soon after the core temperature climbs above 600K. In the blue plots, this occurs less than 2 hours into the scenario, while in the red plots this occurs more than 5 hours into the scenario. This divergence is due to success of the realignment action, which is attempted when the core temperature first reaches 600K. If this action is successful, the AFW system is restored. The restoration of the AFW system recreates a path to reject heat from the reactor core and causes the core inlet temperature to decrease.

When the AFW system is restored due to FLEX, 8 hours into the scenario, the core again has a path for decay heat rejection and the temperature of the primary coolant decreases. This event is easiest to observe in the plots marked in red, where there is a split in the core temperatures shortly beyond 8 hours into the scenario. If FLEX restored cooling, the core temperatures began to slowly decrease from over 600K to above 500K at the end of the simulation time. If instead FLEX was unavailable, the dryout process completed and reactor core temperatures spiked around 9 hours into the scenario. For sequences where the AFW is not restored, however, the core inlet temperatures do not continue increasing. These temperatures remain constant for several hours beyond the onset of core damage (between 7.2 and 9 hours into the scenario) as the primary coolant boils.

This behavior, where coolant in the reactor core takes several hours to completely boil, can be more easily seen by examining an individual sequence. Consequences of sequence #TCDF are shown in Figure 7-10 with the time of important events marked. The AFW is lost 2 hours into the scenario, causing the core temperature to begin to rise. The coolant reaches saturation temperature soon after the realignment action fails and begins to boil 4.69 hours into the scenario, uncovering the core. As the water level in the core drops, the exposed cladding oxidizes and loses integrity, with the onset of this damage occurring 7.334 hours into the scenario. FLEX secures a new AFW supply and restores secondary cooling 8 hours into the scenario. However, the core temperature does not begin to decrease until 8.78 hours into the scenario, over 40 minutes after FLEX is enacted. While restoring the AFW refills the steam generators on the secondary side, the

reactor core temperature does not begin to drop until the primary coolant can reject sufficient heat to the secondary side to begin to reflood the core.

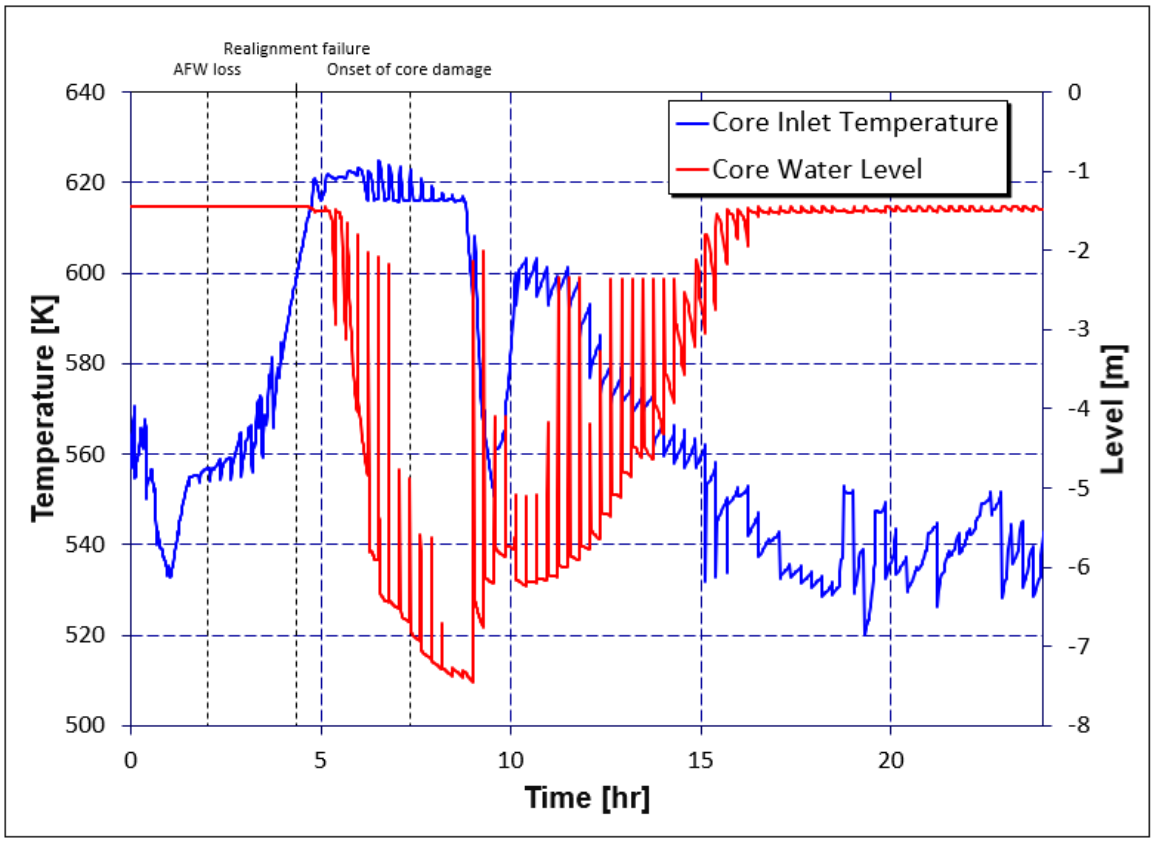


Figure 7-10 Core evolution for sequence #TCDF

Note that the regular spikes that can be observed in the water level are not physical. Instead, they are due to a numerical error that occurs on loading a saved MELCOR file. This occurs alongside momentary errors in the core temperature. A fuller examination of this behavior is described in Section 7.4.4.

### 7.4.3 Integrated Safety-Security Analysis

In addition to the timings of events during the accident sequence, the severity of damage to the reactor and the attendant release of radionuclides were examined. Figure

7-11 shows the fraction of undamaged cladding for all sequences. This damage is primarily caused by oxidation of the cladding material and serves as a proxy for the extent of core damage.

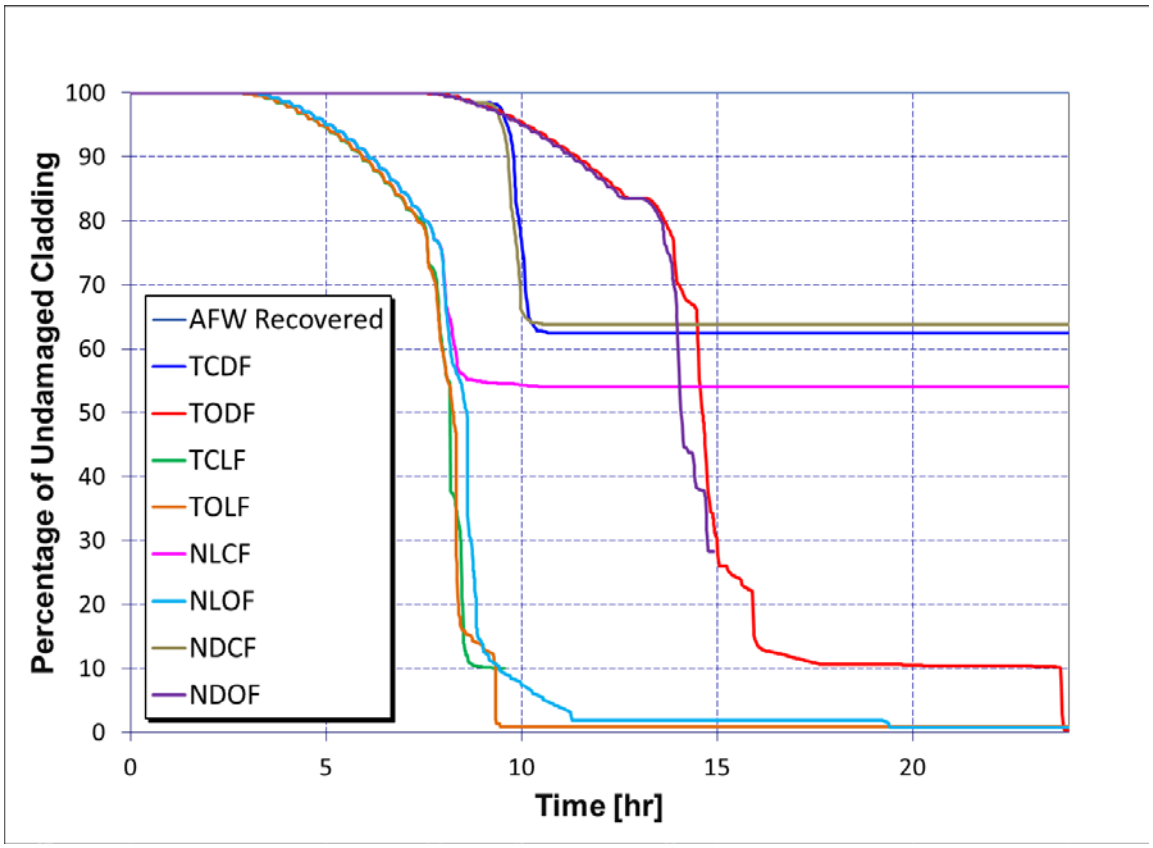


Figure 7-11 Damage to cladding for all sequences (Sequence names based on Table 7-3)

Again, no core damage is observed if operators are successful in performing the mitigating action of realigning the RWST to the AFW system In Figure 7-11, these sequences are collected into the "AFW Recovered" line, which remains at 100% undamaged cladding throughout the simulation. This can also be seen from Table 7-3, which shows that core damage was not observed for any sequence where the realignment action succeeded (All sequences ending with "S"). For sequences where the CST is lost

(those which include the short name “L” from Table 7-2 in the sequence name) over half of the core is damaged between 7.5 and 8.5 hours into the scenario. This damage is delayed for several hours if the CST is instead degraded (sequences which include a “D”), occurring beyond 9 hours into the scenario. Notably, when adversaries are not detected in a timely manner and the CST is lost (in sequences beginning with “NL-”) the accident sequence evolves approximately 10 minutes more slowly than if adversaries are detected (the “TCL-” and “TOL-” sequences). As a result, FLEX is able to reduce the degree of damage to the reactor substantially in sequence #NLCF, compared to sequence #TCLF. Sequence #NLCF keeps under 55% of its cladding from being damaged, while sequence #TCLF recovers with approximately 10% of its cladding remaining undamaged (Note that this sequence crashed soon after recovery).

The release of cesium iodide (CsI) into containment, used as a proxy for the radionuclide release, is shown for all sequences in Figure 7-12. The release into containment is used as a proxy for the radionuclide release rather than the environmental release because even in the most extreme release, belonging to sequence #TODF, the total CsI release to the environment is less than 15 g.

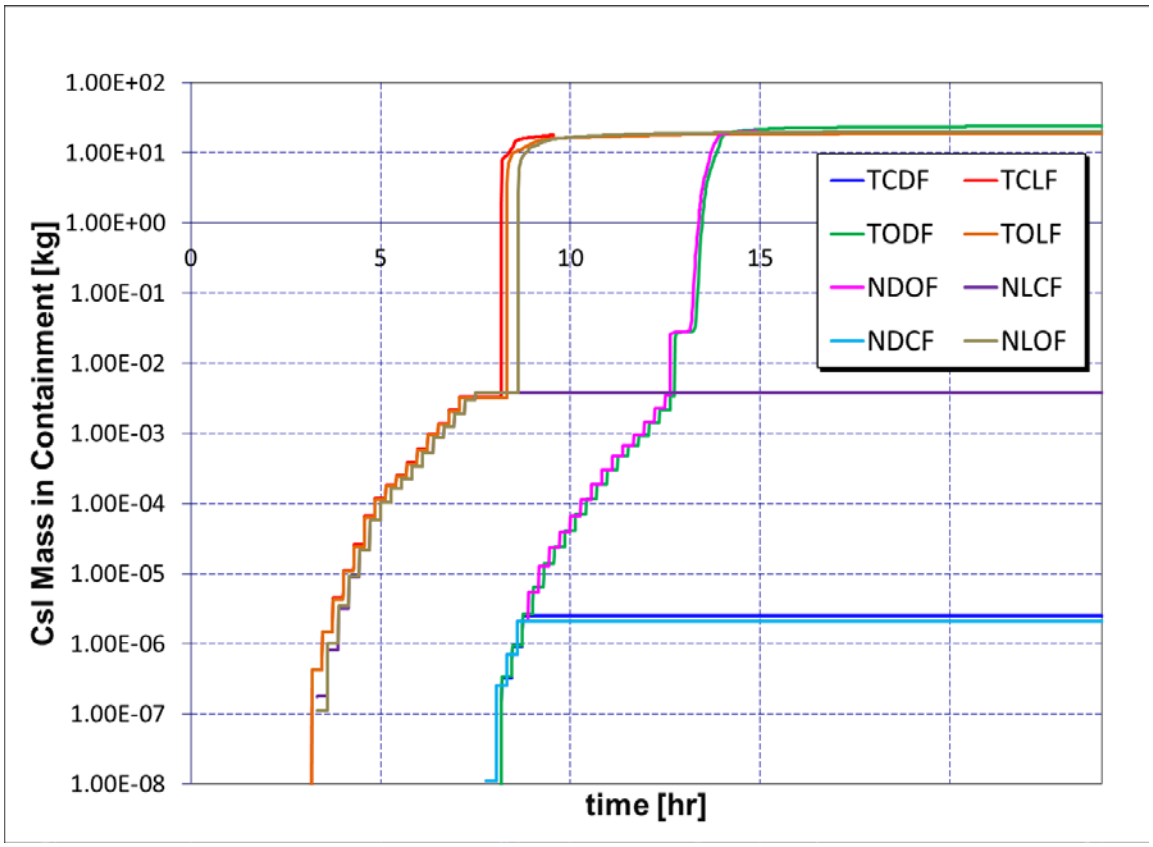


Figure 7-12 CSI release into containment for sequences with core damage (Sequence names based on Table 7-3)

The levels of radiological release can be divided into sequences that are mitigated by FLEX and unmitigated cases, referring to the BCs in Table 7-2. Cases where the operators successfully realign the RWST to the AFW system are not shown in Figure 7-12, as those sequences experience no core damage and therefore no radionuclide release. The remaining cases span nearly 6 orders of magnitude difference in the CsI releases to containment at the end of the scenario (from $10^{-6}$ kg to nearly 20 kg).

When the CST is destroyed by adversaries, the implementation of FLEX is less able to mitigate the amount of radiological release. In sequence #TCLF in Figure 7-12, a total of 17.91kg of CsI were released into containment, compared to 19.04kg if FLEX

was not implemented as in sequence #TOLF (see Row 8 in Table 7-3). In sequence #NLCF, however, there is a 10 minute delay in the accident timeline compared to sequence #TCLF. This delay allows FLEX to have a greater mitigating effect. This difference in the accident sequence timing can be seen in Table 7-3, and in sequence #NLCF only 3.7g of CsI were released in total. Sequence #TCLF, however, resulted in a total release of 17.9kg CsI to the containment structure. Sequences #NLCF and #TCLF split approximately 8.5 hours into the scenario. Sequence #TCLF releases the bulk of the total CsI released during the sequence at this time, while FLEX prevented this release from occurring in sequence #NLCF. These results demonstrate that the consequences of Case Study 3 can be highly sensitive to small changes in the timing of events in the modeled scenario.

### 7.4.4 Time Block Sensitivity

Upon loading a saved MELCOR restart file, the reactor coolant temperature and liquid level experience momentary spikes. These spikes appear to be the result of an error in the save and load process of MELCOR and do not represent any physical phenomena occurring in the reactor. To examine these effects, a sensitivity analysis on the effects of different length time blocks was performed. The length of time between CST sabotage and the operator realignment BCs in sequence #TCDF was used for this purpose.

Successive analyses of this period with increasing time block lengths were performed. These analyses began with a time block of 125 seconds and doubled for each successive analysis. This resulted in time blocks ranging from 125 to 16,000 seconds in

length, and the time to reach the operator realignment BC for each of these time block lengths is shown in Figure 7-13.

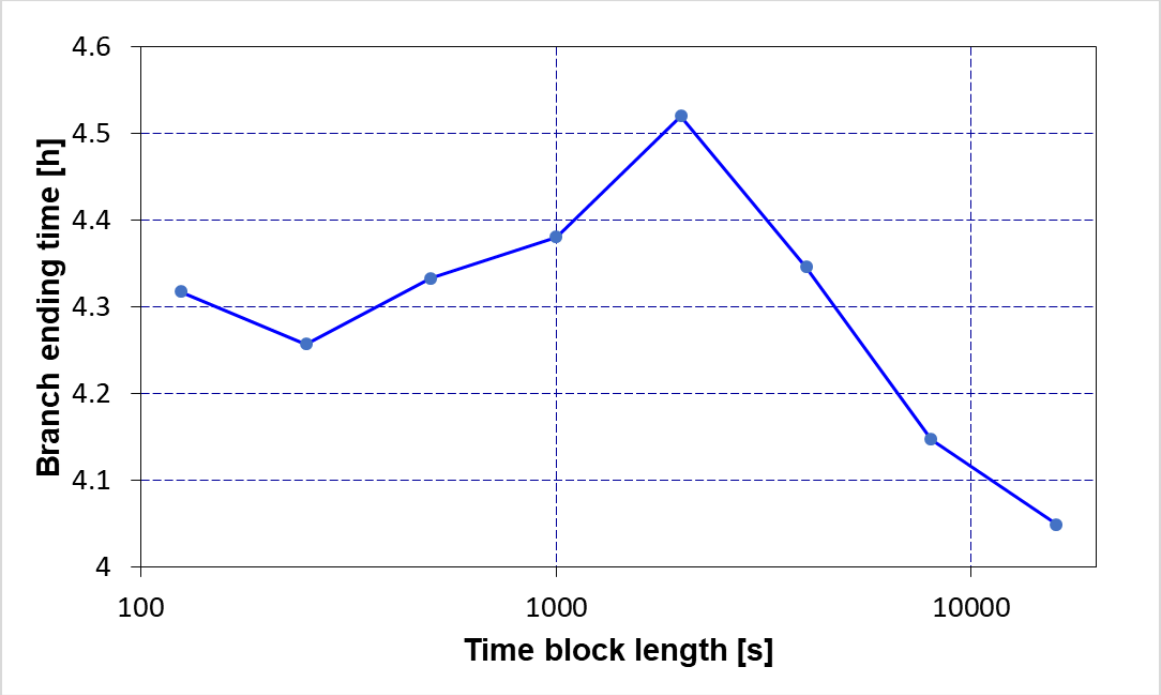


Figure 7-13 Operator realignment time for sequence #TCDF

The length of time in sequence #TCDF between sabotage of the CST and the branching condition for high core temperature is less than 16,000 seconds. Therefore, when the time block length is set this high, the MELCOR simulation runs between BCs without pause. For this sensitivity analysis, the parameter of interest is the time taken to reach the high core temperature BC, which occurs when the core inlet temperature reaches 600K. The process of reloading MELCOR though the LS/TS method delays the occurrence of the high core inlet temperature BC by up to half an hour or 1800 seconds for a time block of 2000s.

These results show that reloading MELCOR through the LS/TS methodology has an effect on the accident sequence evolution. However, the cause of this error is due to the spiking in the core temperature and water level that were observed in Figure 7-10. Different system codes, depending on their construction and possible errors that occur on saving and reloading the code, may experience no dependency on the time block length or different dependency profiles. The determination of these effects is left as future work, described more fully in Section 8.3.2.

## 7.5 Conclusion

Case Study 3 illustrates an integrated safety-security analysis on a NPP using the LS/TS methodology. The scenario used for this analysis is one that, using standard VAI, is assumed to result in an unacceptable release of radionuclides, due to the successful sabotage of a complete target set, including the CST vital area. However, the LS/TS analysis determined that this may be an overly conservative result. Depending on the amount of damage caused by adversaries, there are several hours available to LPNPP operators to regain control of the plant and implement mitigating actions. Table 7-3 shows that if the CDT is degraded by adversaries, the onset of core damage occurs more than 7 hours into the scenario (see rows 2, 6, 10, and 14).

Additionally, the results presented in Table 7-3 show that core damage can be completely averted by the success of the operator action to align the RWST with the AFW system. Therefore, adversaries must additionally prevent this action in order to achieve core damage. Recall that target sets are combinations of locations that contain SSCs which must all be sabotaged to achieve core damage. The results of this modeling,

which show that the operator action of realigning the RWST with the AFW system is sufficient to avert core damage, demonstrate that the adversary target set should be expanded to include adversaries preventing this mitigation action. These results also suggest that the security of the NPP may be improved by allowing operators to realign the RWST with the AFW system from the CR, instead of needing to perform a field action to do so.

The FLEX system greatly reduces the degree of core damage that occurs if the CST was degraded rather than destroyed, as shown in Figure 7-12. In the scenario constructed for Case Study 3, as stated in Section 7.4.3, use of FLEX equipment reduces the radionuclide release by nearly 6 orders of magnitude, and could result in release below regulatory limits. If the CST is destroyed, implementing FLEX at 8 hours may have a limited impact on the radionuclide release, despite a large degree of this release occurring after 8.5 hours into the scenario (compare sequences #NLCF and #TCLF). In this case study, FLEX is restoring secondary cooling despite the reactor core being uncovered. This limited impact implies that a different FLEX action which supplies coolant to the reactor core may affect the core temperature more quickly and be more effective at halting the accident evolution.

Since it is used to illustrate the capabilities of the LS/TS methodology only and not to draw conclusions for an actual attack on a critical facility, there are some limitations to Case Study 3. In this scenario, adversaries defeat the onsite response force several hours before offsite responders arrive. While adversaries in this scenario use this time to interdict operator actions, there may be other sabotage actions adversaries could

perform during this time. Additionally, despite this case study determining the effects of sabotage to SSCs, it does not present a systematic method to identify new target sets. Operator actions or systems that were not modeled in this case study could also affect the scenario.

# Chapter 8 – Conclusion

This dissertation introduces the novel LS/TS methodology, which is an enhancement of the DET approach to enable the approach to manage multiple simultaneous integrated system codes due to the challenges of the current ADAPT multisimulator structure when simulators are sunning simultaneously (Section 6.2). Case Study 1 was performed to conduct a 2S analysis using the current state of the art and demonstrated some of the limitations of the traditional DET methodology. Case Studies 2 and 3 were performed using the newly-developed LS/TS methodology and demonstrated the viability of the LS/TS methodology, as well as the ability for this methodology to be used to support integrated 2S analysis.

Concluding remarks on advantages of the LS/TS methodology to support integrated analyses are presented in Sections 8.1 and 8.2. Limitations of this methodology and unexplored avenues of research are left for future work and described in Section 8.3.

## 8.1 Integrated Safety and Security Phenomena

The LS/TS methodology allows analysts to create scenarios that incorporate simultaneous and interdependent phenomena, even if these phenomena are modeled by separate codes. Information can be passed as necessary and at appropriate times during the simulation by the DET driver. In addition, as multiple simulators are driven in a

systematic fashion using the LS/TS methodology, the analyst does not need to preselect which simulator is run after each BC. In the event of a race condition, where phenomena are developing in multiple simulators that may lead to incompatible BCs, the LS/TS methodology ensures that the earlier BC will be applied and affect the plant state at the appropriate time.

These capabilities are necessary to conduct an integrated 2S analysis using DPRA. To perform an integrated 2S analysis, the performance of the PPS, including the timing and extent of damage to a NPP, affects and is affected by the reactor response. The loss of one system may increase the demand on other systems and change which systems are the most necessary to protect. In addition, FLEX and SAFER equipment allows for a protection strategy of delay rather than defeat of adversaries, which requires security analysis to include the dynamics of accident evolutions.

Case Study 1 demonstrates the interconnected nature of safety and security for a SNF transportation scenario. Tension between safety and security could be seen from the BC on LLE notification, shown in Table 6-1. The modeled effects in Table 6-1 of providing advanced notice to LLE contrasted more rapid evacuation of the public in the event of an accident (under RADTRAN effects) with the possibility of a larger adversary attack (under STAGE effects). The use of DPRA is able to highlight the effects of this decision on the overall risk, as described in Section 6.1.2. In addition, this case study demonstrates the limitations of the current state of the art for DET branching among multiple simulators in a simulator-agnostic manner, as the use of DET branching required

the modeled scenario to separate the safety and security analyses with explicit crossover points during the analysis.

Case Study 2 demonstrates the LS/TS methodology on a simple scenario. This scenario is not one that could be performed using previously existing ADAPT capabilities to combine multiple simulators into one DET. In addition, Case Study 2 demonstrated that the LS/TS method using two simulations can achieve similar results as running the scenario as single simulation and hence verified the LS/TS method.

Case Study 3 uses the LS/TS methodology to perform an integrated 2S analysis of a LWR for the first time. This analysis cannot be cleanly split into separate safety and security analyses as both disciplines within this analysis affect the other discipline. Additionally, the ordering of events in this scenario is not consistent among sequences. Therefore, the simulator of interest for each BC may not be consistent, which would challenge DET branching. The case study, however, demonstrates how to manage such a possible inconsistency, expanding the scope of phenomena that can be handled in a DET and enabling a fuller set of interrelated systems that can be modeled using DPRA.

## 8.2 Dynamic Target Set Analysis

In Section 7.4.3, this work demonstrated that a target set created by the VAI process for LPNPP did not include the full suite of SSCs that needed to be sabotaged in order to result in core damage. Additionally, while the FLEX system did not avert core damage, it successfully reduced the level of damage in the core and the associated release for some branches. Thus Case Study 3 shows that DPRA is capable of evaluating target sets to find out if a given target set is complete and the loss of the included SSCs to

adversaries would result in core damage or a radiological release. In addition, the LS/TS methodology is able to identify potential SSCs for a given target set that may mitigate the consequences of sabotage to the reactor, even if some level of damage occurs (Section 7.4.3). These SSCs may be worth protecting even if the target set cannot be protected to minimize public consequences of reactor sabotage.

Using DPRA to perform an integrated 2S analysis was additionally shown to allow the analyst to identify the radiological release associated with different sabotage scenarios (Section 7.4.3). The addition of more detailed consequence information with sabotage scenarios allows for a fuller understanding of the security risks and provides an opportunity for the PPS to better prioritize limited protection resources following the principle of a "graded approach" as mentioned in Section 2.3. For example, it may be correct to provide one target set that results in damage to 1% of the reactor core and no release and a different target set that releases a large fraction of the reactor core to the environment with different levels of protection, even though adversaries sabotaging either of these target sets results in core damage.

## 8.3 Future Work

As a result of this work, a number of directions for further development of the LS/TS methodology have been identified as indicated in Sections 8.3.1 and 8.3.2 below.

### 8.3.1 Systematic Identification of Target Sets

The case studies used with the LS/TS methodology included a limited number of BCs for the proof of concept of the LS/TS methodology. Subsequently, the full set of uncertainties associated with the scenario under consideration were not considered. For

example, no operator actions that could be performed within the CR, including the implementation of feed and bleed or depressurizing the core to use coolant stored in the accumulators, were considered in Case Study 3. In addition, as mentioned in Section 7.5, adversaries do not attempt to sabotage targets of opportunity after completing their objectives. Including such actions and uncertainties may have a substantial effect on the system response, particularly in the timing of the accident evolution and the effects of mitigation actions and increase the realism of the results.

Including operator procedures and adversary behaviors that involve sabotaging targets of opportunity could allow analysts to get a fuller understanding of the resilience of the NPP. For some scenarios, operator actions alone may protect the core following sabotage of equipment. Similarly, opportunistic sabotage of equipment may result in more severe consequences than were otherwise predicted. Considering this information may result in a more resilient PPS than would otherwise be constructed.

Stochastic failures of equipment were not considered in this analysis. Including these failures into future analyses may identify unexpected sequences that result in negative consequences. Additionally, as adversaries may be able to cause failures equivalent to those arising from stochastic equipment failure, the inclusion of these BCs in DPRA may result in a more complete understanding of a NPP's target sets than would be obtained otherwise.

### 8.3.2 Time Block Optimization

The LS/TS analyses in this work were performed manually and at a small scale. As a result, the computation time required for time blocks of different lengths were not

considered. However, a detailed analysis of an existing plant would require using far more branches than were included in this analysis to cover the risk space in sufficient detail. Both the process of saving and loading a simulator and the potential for the LS to model a moot system state represent computational losses. These losses will also depend on the codes linked through the LS/TS methodology, as different codes have different run speeds and loading times. As the scale of a LS/TS analysis increases, the effects of these losses may become significant. Therefore, the development of a methodology which determines an appropriate time block length, either for the entire analysis or for a given branch, may reduce the computational burden associated with the LS/TS methodology and allow for its more widespread adoption.

# Bibliography


[1] D. Kim and J. Kang, "Where Nuclear Safety and Security Meet," *Bulletin of the Atomic Scientists,* vol. 68, no. 1, pp. 86-93, 2012.

[2] T. Aldemir, "A Survey of Dynamic Methodologies for Probabilistic Safety Assessment of Nuclear Power Plants," *Annals of Nuclear Energy,* vol. 53, pp. 113-124, 2013.

[3] L. Humphries, B. Beeny, F. Gelbard, D. Louie and J. Phillips, "MELCOR Computer Code Manuals (SAND2017-0455)," Sandia National Laboratories, Albuquerque, 2017.

[4] the RELAP5 Development Team, "RELAP5/MOD3 Code Manual (NUREG/CR-5535)," Idaho National Engineering Laboratory, Idaho Falls, 1995.

[5] Z. Jankovsky, M. Denman and T. Aldemir, "Extension of the ADAPT Framework for Multiple Simulators," in *Transactions of the American Nuclear Society*, Las Vegas, NV, 2016.

[6] M. Garcia, "Design and Evaluation of Physical Protection Systems," in *The Design and Evaluation of Physical Protection Systems: Second Edition*, New York, Elsevier, 2008, pp. 1-13.

[7] *68 Stat. 919.*

[8] U.S. Nuclear Regulatory Commission, "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement. 60 FR 42622," U.S. Nuclear Regulatory Commission, Washington, D.C., 1995.

[9] U.S. Nuclear Regulatory Commission, "Reactor safety study. An assessment of accident risks in U. S. commercial nuclear power plants. (WASH-1400)," USNRC, Washington, D.C., 1975.

[10] M. Rogovin, G. Frampton and e. al., "Three Mile Island: A Report to the Commissioners and the Public; Volume 1," Nuclear Regulatory Commission Special Inquiry Group, Washington, D.C., 1980.

[11] "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Industrial Sabotage," *42 Fed. Reg.,* p. 10838, 24 February 1977.

[12] "General Performance Requirements," *42 Fed. Reg.,* p. 34313, 05 July 1977.

[13] G. Varnado and N. Ortiz, "Fault Tree Analysis for Vital Area Identification NUREG/CR-0809," Sandia National Laboratories, Albuquerque, 1979.

[14] T. Bott and W. Thomas, "Reactor Vital Equipment Determination Techniques," in *11th WRSR Information Meeting*, 1983.

[15] J. Boudreau and R. Haarman, "Reactor Sabotage Vulnerability and Vital-Equipment Identification," in *Tenth Water Reactor Safety Research Information Meeting*, Washington, DC, 1982.

[16] D. Cameron, "Vital Areas at Nuclear Power Plants," in *7th International System Safety Conference*, San Jose, 1985.

[17] W. Travers, *Recommendations of the Safeguards Performance Assessment Task Force*, Washington, D.C.: United States Nuclear Regulatory Commission, 1999.

[18] S. Collins, *Order Modifying Licenses (Effective Immediately)*, EA-02-026: NRC, 2002.

[19] U.S. Nuclear Regulatory Commission, *Interim Staff Guidance Compliance with 10 CFR 50.54(hh)(2) and 10 CFR 52.80(d) Loss of Large Areas of the Plant due to Explosions or Fires from a Beyond-Design Basis Event.*

[20] G. Varnado and D. Whitehead, "Vital Area Identification for U.S. Nuclear Regulatory Commission Nuclear Power Reactor Licensees and New Reactor Applicants SAND2008-5644," Sandia National Laboratories, Albuquerque, 2008.

[21] T. Malachova, J. Malach and Z. Vintr, "Threat Characterization in Vital Area Identification Process," in *47th International Carnahan Conference on Security Technology (ICCST)*, Medellin, 2013.

[22] International Atomic Energy Agency, "Convention on the Physical Protection of Nuclear Materials," Vienna, 1979.

[23] International Atomic Energy Agency, "Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20," IAEA, Vienna, 2013.

[24] International Atomic Energy Agency, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13," IAEA, Vienna, 2011.

[25] United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73 Section 55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage," [Online]. Available: https://www.nrc.gov/reading/rm/doc-collections/cfr/part073/part073-0055.html.

[26] M. Benson, "Overview of Physical Protection Systems Design and Evaluation," Sandia National Laboratories, Albuquerque, 2013.

[27] J. Williams, "DOE/SS Handbooks-A Means of Disseminating Physical Security Equipment Information," *Journal of the Institute of Nuclear Materials Management*, vol. 7, no. 1, pp. 65-76, 1978.

[28] M. Garcia, "Determining System Objectives," in *The Design and Evaluation of Physical Protection Systems: Second Edition*, New York, Elsevier, 2008, pp. 13-55.

[29] United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73, "Physical Protection of Plants and Materials," [Online]. Available: https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/.

[30] U.S. Nuclear Regulatory Commission, "Seismic Design Classification for Nuclear Power Plants (RG 1.29)," U.S. Nuclear Regulatory Commission, Washington, D.C., 2016.

[31] M. Shackelford, T. Bump and R. Seidensticker, "Characterization of Nuclear Reactor Containment Penetrations Final Report," Argonne National Laboratories, Argonne, 1985.

[32] M. Garcia, Vulnerability Assessment of Physical Protection Systems, New York: Elsevier, 2006.

[33] M. Garcia, "Analysis and Evaluation," in *The Design and Evaluation of Physical Protection Systems: Second Edition*, New York, Elsevier, 2008, pp. 261-299.

[34] Lawrence Livermore National Laboratory, "Joint Conflict and Tactical Simulation (JCATS) Capabilities Brief," Lawrence Livermore National Laboratory, Livermore, 2018.

[35] B. Hart, D. Hart, R. Gayle, F. Oppel, P. Xavier and J. Whetzel, "Dante Agent Architecture for Force-On-Force Wargame Simulation and Training," in *The Thirteenth AAAI Conference on Artificial Intelligence and Interactive Digital Entertainment*, Snowbird. UT, 2017.

[36] United States Nuclear Regulatory Commission, "Frequently Asked Questions About Force-on-Force Security Inspections at Nuclear Power Plants," 31 March 2020. [Online]. Available: https://www.nrc.gov/security/faq-force-on-force.html. [Accessed 05 October 2020].

[37] S. Kaplan and B. Garrick, "On the Quantitative Definition of Risk," *Risk Analysis,* vol. 1, no. 1, 1981.

[38] W. Vesely, F. Goldberg and e. al., "Fault Tree Handbook (NUREG-0492)," United States Nuclear Regulatory Commission, Washington, D.C., 1981.

[39] C. Udell, J. Tilden and R. Toyooka, "Modified Risk Evaluation Method," in *Institute of Nuclear Materials Management 34th Annual Meeting*, Scottsdale, 1993.

[40] G. Apostolakis and D. Lemon, "A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities due to Terrorism," *Risk Analysis,* vol. 25, no. 2, pp. 361-376, 2005.

[41] N. Khakzad, G. Reniers and P. Gelder, "A Multi-Criteria Decision Making Approach to Security Assessment of Hazardous Facilities," *Journal of Loss Prevention in the Process Industries,* vol. 48, pp. 234-243, 2017.

[42] D. Fakhravar, N. Khakzad, G. Reniers and V. Cozzani, "Security Vulnerability Assessments of Gas Pipelines Using Discrete-Time Bayesian Network," *Process Safety and Environmental Protection,* vol. 111, pp. 714-725, 2017.

[43] F. Durán, G. Wyss, S. Jordan and B. Cipiti, "Risk-Informed Management of Enterprise Security: Methodology and Applications for Nuclear Facilities," in

*International Conference on Nuclear Security: Enhancing Global Efforts*, Vienna, 2014.

[44] D. Moore, B. Fuller, M. Hazzan and J. Jones, "Development of a security vulnerability assessment process for the RAMCAP chemical sector," *Journal of Hazardous Materials*, vol. 142, no. 3, pp. 689-694, 2007.

[45] J. Brashear and J. Jones, "Risk Analysis and Management for Critical Asset Protection (RAMCAP Plus)," in *Wiley Handbook of Science and Technology for Homeland Security*, 2010.

[46] A. Cipollaro and G. Lomonaco, "Contributing to the nuclear 3S's via a methodology aiming at enhancing the synergies between nuclear security and safety," *Progress in Nuclear Energy*, vol. 86, pp. 31-39, 2016.

[47] M. Stein and M. Morichi, "Safety, Security, and Safeguards by Design: An Industrial Approach," *Nuclear Technology*, vol. 179, no. 1, pp. 150-155, 2012.

[48] International Nuclear Safety Group, "The Interface Between Safety and Security at Nuclear Power Plants (INSAG-24)," International Atomic Energy Agency, Vienna, 2010.

[49] D. Osborn, *Integrated Safety-Security Methodology for Loss of Large Area Analysis*, Singapore: Sandia National Laboratories, 2017.

[50] G. Parnell, C. Smith and F. Moxley, "Intelligent Adversary Risk Analysis: A Bioterrorism Risk Management model," *Risk Analysis*, vol. 30, no. 1, pp. 32-48, 2010.

[51] S. Contini, G. Cojazzi and G. Renda, "On the use of non-coherent fault trees in safety and security studies," *Reliability Engineering & System Safety*, vol. 93, no. 12, pp. 1886-1895, 2008.

[52] S. Gandhi and J. Kang, "Nuclear Safety and Nuclear Security Synergy," *Annals of Nuclear Energy*, vol. 60, pp. 357-361, 2013.

[53] N. Zakariya and M. Kahn, "Safety, Security and Safeguard," *Annals of Nuclear Energy*, vol. 75, pp. 292-302, 2015.

[54] L. Cox, "Improving Risk-Based Decision Making for Terrorism Applications," *Risk Analysis*, vol. 29, no. 3, pp. 336-341, 2009.

[55] B. Ezell, S. Bennett, D. Winterfeldt, J. Sokolowski and A. Collins, "Probabilistic Risk Analysis and Terrorism Risk," *Risk Analysis*, vol. 30, no. 4, pp. 575-589, 2010.

[56] G. Brown and L. Cox, "How Probabilistic Risk Assessment Can Mislead Terrorism Risk Analysis," *Risk Analysis*, vol. 31, no. 2, pp. 196-204, 2011.

[57] B. Ezell and A. Collins, "Letter to the Editor," *Risk Analysis*, vol. 31, no. 2, p. 192, 2011.

[58] G. Brown and L. Cox, "Making Terrorism Risk Analysis Less Harmful and More Useful: Another Try," *Risk Analysis*, vol. 31, no. 2, pp. 193-195, 2011.

[59] L. Cox, "Some Limitations of "Risk = Threat x Vulnerability x Consequence" for Risk Analysis of Terrorist Attacks," *Risk Analysis*, vol. 28, no. 6, pp. 1749-1761,

2008.

[60] E. Strickland, "24 Hours at Fukushima," *IEEE Spectrum,* 31 October 2011.

[61] E. Gottlieb, R. Harrigan, M. McDonald, F. Oppel and P. Xavier, "The Umbra Simulation Framework," Sandia National Laboratories, Albuquerque, 2001.

[62] T. Le, J. Parks and T. Noel, "Mixed Reality 3D Tabletop Tool with Radioactive Source Model Visualization," in *International Conference on the Security of Radioactive Material: The Way Forward for Prevention and Detection*, Vienna, 2018.

[63] Presagis, "STAGE Scenario Technical Overview," Presagis, Montreal, 2008.

[64] M. Snell, J. Rivers and D. Shull, "Summary of Analysis Methodology Results of the Nuclear Security Assessment Methodologies (NUSAM) Coordinated Research Project," International Atomic Energy Agency, Vienna, 2017.

[65] Unity Technologies, [Online]. Available: www.unity.com. [Accessed 13 October 2020].

[66] Electric Power Research Institute, "Use of MAAP in Support of Post-Fukushima Applications," Electric Power Research Institute, Palo Alto, 2013.

[67] R. Weiner, K. Neuhauser, T. Heames, B. O'Donnell and M. Dennis, "RADTRAN 6 Technical Manual," Sandia National Laboratories, Albuquerque, 2014.

[68] Z. Jankovsky, T. Haskin and M. Denman, "How to ADAPT," Sandia National Laboratories, Albuquerque, 2018.

[69] G. Cojazzi, "The DYLAM Approach for the Dynamic Reliability Analysis of Systems," *Reliability Engineering and System Safety,* vol. 52, pp. 279-296, 1996.

[70] M. Kloos and J. Peschke, "MCDET: A Probabilistic Dynamics Method Combining Monte Carlo Simulation with the Discrete Dynamic Event Tree Approach," *Nuclear Science and Engineering,* vol. 153, no. 2, pp. 137-156, 2006.

[71] C. Queral, J. Gómez-Magán, J. Rivas-Lewicky, M. Sánchez-Perea, C. Paris, J. Gil, J. Mula, E. Meléndez, J. Hortal, J. Izquierdo and I. Fernández, "Dynamic Event Trees without Success Criteria for Full Spectrum LOCA Sequences applying the Integrated Safety Assessment Methodology," *Reliability Engineering & System Safety,* vol. 171, pp. 152-168, 2018.

[72] Y. Chang and A. Mosleh, "Cognitive Modeling and Dynamic Probabilistic Simulation of Operating Crew Response to Complex System Accidents Part 5: Dynamic Probabilistic Simulation of the IDAC Model," *Reliability Engineering and System Safety,* vol. 92, pp. 1076-1101, 2007.

[73] Idaho National Laboratory, "EMRALD," [Online]. Available: https://emrald.inl.gov. [Accessed 07 October 2020].

[74] R. O'Keefe, "The Three-Phase Approach: A Comment on Strategy-Related Characteristics of Discrete-Event Languages and Models," *Simulation,* vol. 47, no. 5, 1986.

[75] A. Williams, D. Osborn, K. Jones, E. Kalinina, B. Cohn, A. Mohagheghi, M.

DeMenno, M. Thomas, M. Parks, E. Parks and B. Jeantete, "System Theoretic Frameworks for Mitigating Risk Complexity in the Nuclear Fuel Cycle SAND2017-10243," Sandia National Laboratories, Albuquerque, 2017.

[76] D. Osborn, M. J. Parks, R. Knudsen, K. Ross, C. Faucett, T. Haskin, P. Kitsos, T. Noel and B. Cohn, "Modeling for Existing Nuclear Power Plant Security Regime (SAND2019-12015)," Sandia National Laboratories, Albuquerque, 2019.

[77] M. Garcia, "Design Physical Protection System," in *The Design and Evaluation of Physical Protection Systems: Second Edition*, New York, Elsevier, 2008, pp. 55-261.

[78] T. Goolsby, "Access Delay Design Principles," in *Integrated Security Design Workshop*, Albuquerque, 2013.

[79] U.S. Nuclear Regulatory Commission, "Probabilistic Risk Assessment (PRA)," 04 January 2018. [Online]. Available: https://www.nrc.gov/about-nrc/regulatory/risk-informed/pra.html. [Accessed 04 October 2020].

# Appendix A - Overview of PPS Design

A PPS is commonly divided into three separate elements; those being detection, delay and response [77]. These elements interact to ensure that the DBT adversary will be interrupted and neutralized before they are able to complete all of their tasks. To achieve these objectives, it is necessary that adversaries are sufficiently delayed *after* the time of first detection such that the response can prepare itself and arrive. As no system can be known to work with complete effectiveness, a number of design principles are commonly recommended as best practices.

The first PPS design best practice is to use protection-in-depth [77]; akin in safety assessments a defense-in-depth. This concept uses multiple and diverse protective layers at the NPP site that must each be breached or defeated in turn by an adversary. This has several advantages to this approach, for example;

- Building several layers of detection requires an adversary to defeat each layer in turn if that adversary is attempting to use stealth.
- If the PPS detection and delay layers are diverse, and cannot all be defeated in similar ways, then the adversaries will need the necessary equipment and capabilities to succeed at all steps to defeat the varied strategies. If adversaries are unable to defeat any of these layers, then the overall goal of facility security will be achieved.

- If there are multiple types of delay barriers adversaries would need to cross, adversaries would need to gather enough information and tools to defeat each barrier in turn, and risk failing at each barrier.

Another best practice is to minimize the negative consequences of any single component failure [77]. This practice is philosophically similar to the single failure criterion in safety analysis and concedes that the PPS will inevitably have failures of any systems or components that are relied upon. Especially given the possibility of adversary action destroying PPS components, contingency plans or backup systems that can ensure the continuity of PPS operations add a great deal of resilience to the system.

The last major best practice is to ensure that the protection is balanced for all potential adversary paths [77]. This means that regardless of the adversary's planned route, they will encounter equivalent levels of detection, delay and response. Importantly, adversary pathways do not need to go through ordinarily traversable terrain. For example, in order to enter a room, adversaries can travel through windows and doors, but walls, ceilings, floors, and vents are all possible pathways that need to be protected. Similarly, if a door is locked, adversaries can attempt consider not only defeating the lock, but the door, hinges, or doorframe to enter. This best practice does not, however, result in built systems with identical difficulties for all pathways in all circumstances. It is possible that structural or other requirements will give some pathways greater strength against the adversary than others. As long as the most vulnerable path meets the security requirements, it is acceptable if other pathways have greater levels of protection. The elements of a PPS, detection, delay and response, are described in more detail below.

Section A.1 describes detection methods, Section A.2 introduces access delay and Section A.3 describes the response elements of a PPS.

## A.1 Intruder Detection

Intrusion detection systems depend on a number of components and subsystems. These include sensors, alarm assessment, and entry control systems. Intrusion sensors passively or actively observe some location within a site. When some preset condition occurs, the sensor sends an alarm signal, often to the CAS. Alarm assessment is a task that is performed by a human observer (security office) in the event of receipt of an alarm signal. Members of the security organization in the CAS observe the location corresponding to the alarm to determine if the alarm corresponds to an actual event. If the assessment confirms the presence of an adversary, the detection and assessment process is complete. Importantly, the detection process is not complete until an alarm has been correctly assessed as being caused by an adversary. In addition to detecting unauthorized persons in a facility, it is necessary to permit authorized persons to access the facility and perform their appropriate tasks. Entry control systems are how the PPS system determines authorized persons and permits them entry to authorized areas.

In the event of an adversary intrusion, an intrusion sensor is designed to send an alarm detecting the presence of an intruder, which is confirmed by alarm assessment and used to start the PPS response. Ideally, an intrusion sensor would have a probability of detection $P_D$ of 1.00, where the sensor always detects an intruder. However, $P_D$ is calculated based on performance tests, which are unable to guarantee that a sensor will always function as desired. Additionally, while a given installed sensor will have some

true value of $P_D$, this number cannot be known; in the same way that the exact probability of a system malfunctioning can only be estimated. All that can be known is the likelihood that the true value of $P_D$ is greater than some estimation of $P_D$. Therefore, intrusion sensors are tested to estimate $P_D$ with a given confidence level $C_L$, typically 0.90 or above. This means that, based on some number of performance tests of a sensor, the likelihood that the true value of $P_D$ for that sensor is at least the estimated value is 0.90. This is the standard metric used for $P_D$ of intrusion sensors.

The purpose of intruder detection is to detect adversaries as they enter and travel through the site. Exterior intrusion sensors represent the first opportunity for a PPS to detect an adversary attack on an NPP. To fulfill the nuclear security best practice of balanced protection, exterior intrusion sensors are installed in continuous lines around the facility, where the only breaks in coverage are at entry buildings and access control points. To accomplish such a coverage and allow the security organization to know where along the sensor line an alarm occurred, a sensor line is divided into coverage sectors, ensuring that the edges of the sectors overlap to prevent any gaps existing in the sensor coverage.

The first detection layer used for this purpose is the perimeter intrusion detection and assessment system (PIDAS),[4] located on the exterior protected area boundary. The PIDAS consists of two sets of fences with an isolation zone several yards wide between them. This zone is cleared of all vegetation and obstructions. Inside the zone are at least

[4] Domestic NPP security professionals typically call this a PIDS – perimeter intrusion detection system.

two continuous lines of external sensors, following the best practice of protection in depth. These sensors should be complimentary, such that the combination of sensors would be more difficult to defeat than the individual sensors. In order to achieve such a complimentary arrangement, sensors should require different methods to defeat and the tools which could be used to defeat one sensor should be difficult to transport past other sensors.

The effectiveness of exterior sensors depends on the expected NPP site's environment. The environment, particularly the weather, has a substantial effect on the overall effectiveness of an external sensor. Many sensors detect adversaries through changing reflections in the environment or electric fields. Weather, such as rain, can also cause these effects. If this occurs, the sensor will alarm but no intruder will be present when the alarm is assessed. This is called a nuisance alarm, and the exterior sensors need to be designed to a low nuisance alarm rate (NAR) that is within manageable bounds by the CAS. Additionally, a sensor may signal an alarm without the conditions for an alarm being present. Such an alarm is a false alarm and differs from a nuisance alarm. When a sensor gives off a nuisance alarm, the sensor is correctly reporting the conditions of the alarmed area, but the cause is due to the environment and not an intruder. When a sensor gives off a false alarm, the sensor is failing to correctly report on the alarmed area. Therefore, false alarms are an indication of a malfunction in the sensor that requires maintenance. A PPS should identify the causes of false alarms and eliminate their sources whenever feasible.

Interior alarms differ from exterior alarms in a number of important ways. While the basic physics of sensors still apply, interior locations can differ greatly from exterior ones. Typically, interior locations are fully controlled by the facility, and allow for different sensor types. Additionally, the interior environment has a larger number of chokepoints, such as doors and staircases, adversaries are more likely to travel through. This means that in addition to volumetric sensors that detect an adversary traveling through a volume, sensors that detect entrances into rooms can be effective. Another difference is that inside the facility, operators need to move between locations to perform work activities. Interior sensors, during work activities, may need to be less intrusive and changed to an "access" mode where alarms do not get reported to the CAS.

After an alarm signal has been generated, the alarm needs to be assessed to determine if the alarm is due to an intruder or a nuisance or false alarm. This is performed in the CAS where security operators receive the alarm signal. At NPPs, alarm assessment is generally performed with video recordings from dedicated assessment cameras from several seconds before the alarm to several seconds past the alarm. For each coverage sector, typically one dedicated assessment camera is used. These cameras have a fixed view of their coverage sector and are separate from pan tilt zoom cameras that can be used to perform surveillance of the plant. This size of exterior coverage sectors is limited to ensure that the presence of an intruder can be determined from the assessment camera video. Importantly, detection is not considered to have occurred until the adversaries have been successfully assessed.

In addition to detecting alarms from intruders, the detection element of a PPS needs to permit authorized access to and through the facility [77]. Entrance to NPPs is, in general, through dedicated entry control points where one or more security guards are present to scan for contraband and allow access. There are several ways that a NPP can ensure personnel are authorized to enter the facility. These are typically divided into the categories of:

- What you have (e.g. badges);
- What you know (e.g. passwords), and;
- What you are (e.g. biometrics).

For high security applications such as NPPs, best practices in access control recommend that facilities require two or more of these factors to allow entry.

## A.2 Delay

Once an intruder has been detected, an effective PPS needs the adversaries to be delayed from their target for at least as long as it takes for the response force to interrupt the adversary tasks. In order to achieve such a delay, barriers are installed to increase the time adversaries take to accomplish their tasks. However, as the response process does not begin until after adversaries have been detected and assessed, no credit is given for delay until after detection has occurred. Therefore, the outermost delay barriers are typically placed just inside the PIDAS.

Vehicles are a valuable resource for adversaries and can have a substantial effect on their timeline. As the NPP PIDAS is often located away from the adversary targets, delay can be gained from something as simple as the traversal time across the site's

owner-controlled area or limited area. In addition, adversaries often need to make use of heavy or bulky tools but carrying tools on foot slows and tires the adversary, which generally provides a practical limit on the equipment adversaries can afford to carry. If adversaries bring a vehicle onsite, however, they are able to greatly reduce travel times and carry all of their desired equipment in the vehicle.

Best practices for delay recommend that NPPs install vehicle barriers just inside the inner PIDAS fence [78]. These are structures (e.g. bollards) that can be crossed on foot but cannot be crossed by vehicles within the DBT. Such structures force the adversaries to choose between abandoning their vehicles and much of their gear to proceed on foot and dismantling the vehicle barrier to keep the use of their vehicle. In either case, however, the adversary timeline has been delayed.

If perimeter barriers, such as a fence, are installed at the PIDAS as well, this enhances the detection systems. Barriers require adversaries to penetrate the barrier while inside a detection area, which increases the probability of detection and that the adversary will still be at the detection point during assessment. Additionally, installing delay alongside detection has the possibility in assisting the PPS response. If the delay is sufficiently long, the response may interrupt the adversaries while they are near a detection volume where their location is known.

In addition to perimeter barriers, there are other types of adversary delay. Such delays can be divided into two categories: (1) passive measures, and, (2) active measures. Passive measures are delay barriers that always function. These types of barriers include reinforced doors and walls, or tie-downs with chains or wires that need to be removed

before an asset can be accessed. Such barriers have the advantage that they are always available, but operations can also negatively impacted by these barriers.

Active delay barriers are any types of barrier that must be deployed in some fashion to be used, and generally are deployed upon the detection and assessment of an adversary. These barriers include pop-up bollards and dispensable barriers such as deployable smokes or aqueous foams. Dispensable smokes and foams obstruct the adversary by obscuring the environment and make any tasks adversaries need to perform more challenging.

A significant amount of delay can be gained by using multiple and diverse delay barriers as part of the protection in depth philosophy. By using many delay barriers, which need to be penetrated using different methods, the task adversaries have is substantially more difficult. Not only do adversaries need to have developed different methods to defeat each barrier they intend to penetrate, but any tools that the adversary wishes to use against later barriers needs to be carried through all of the previous barriers they penetrate. However, a sufficiently determined individual can eventually penetrate *any* delay barrier. Therefore, some form of intervention will always be necessary to prevent adversaries from accomplishing their tasks.

## A.3 Response

If a security event occurs at a facility, some form of response is necessary. Response is often broken into two categories [77]: (1) timely response, which seeks to interrupt the adversary, and, (2) after-the-fact recovery actions. After-the-fact recovery is

generally used for lower-consequence events where allowing the adversary to accomplish their objective, such as vandalism or commercial store theft, is deemed acceptable.

The form of response that an adversary will require depends on the DBT. For some threats, such as skateboarders trespassing in the facility, either recovery or timely response by an unarmed guard may be sufficient. Others, however, may be attempting to cause major radionuclide releases. If the adversaries are willing to use violence and sufficiently committed to their tasks, it may not be possible to cause adversaries to abandon their attack. For this type of adversary, response requires a timely armed force that can neutralize the adversaries as used in domestic NPPs.

For a response force the most important attributes are the probability of interrupting adversaries ($P_I$) and the probability of neutralizing adversaries given their interruption ($P_N$).

Interruption occurs when the response force arrives in sufficient numbers as to require the adversaries to abandon their current task; this may require one or multiple members of the response force, depending on the type of adversary threat. Neutralization is any type of interaction between the adversary and the response force that causes the adversary to abandon their objective(s).

Both onsite and offsite responses can be used for either timely or after-the-fact response. However, offsite response typically has a longer response timeline due to the necessity of arriving from offsite (i.e., offsite response could be hours). In addition, an offsite responder is unlikely to be as familiar with the site and its layout as an onsite response force. However, an offsite response force can be larger than a site could

maintain for onsite response. Therefore, if an offsite response force is used by a facility, the PPS will either need to include sufficient delay to ensure the offsite response force can arrive or accept that the response will be an after-the-fact response.

# Appendix B - Edit Rules for Case Study 1

```
InputFile 1 RADTRAN.INPUT.tpl          // the "base" template RADTRAN input file with
character variables to be edited by ADAPT
InputFile 2 stage_translator.tpl

StoppingWord 1 RADTRAN.OUTPUT STOPPINGCODE 3       // <filename> <magicword>
<word_on_that_line>
StoppingWord 2 stage_translator MAJTOM 3

VarSeparator 1 "{" "}"                    // These are the brackets that separate the
input varables
VarSeparator 2 "{" "}"

SimulatorExecutable 1 rt6
SimulatorExecutable 2 stage

InitialSimulator 1

// Simulator to be run when each branching code is reached.
BranchingSimulator 01 1
BranchingSimulator 02 1
BranchingSimulator 03 1
BranchingSimulator 04 1
BranchingSimulator 05 1
BranchingSimulator 07 1
BranchingSimulator 10 2

// Probability for each main branch of each branching condition.
BranchProbability 01 1 1/6 // Minimal LLE warning -slow
BranchProbability 01 2 1/6 // Minimal LLE warning -med
BranchProbability 01 3 1/6 // Minimal LLE warning -fast
BranchProbability 01 4 1/6 // Heightened LLE warning -slow
BranchProbability 01 5 1/6 // Heightened LLE warning -med
BranchProbability 01 6 1/6 // Heightened LLE warning -fast

BranchProbability 02 1 0.041666 // Inventory
BranchProbability 02 2 0.041667
BranchProbability 02 3 0.041667
BranchProbability 02 4 0.041666
BranchProbability 02 5 0.041667
BranchProbability 02 6 0.041667
BranchProbability 02 7 0.041666
BranchProbability 02 8 0.041667
BranchProbability 02 9 0.041667
BranchProbability 02 10 0.041666
BranchProbability 02 11 0.041667
BranchProbability 02 12 0.041667
BranchProbability 02 13 0.041666 // Cut to 12 branches to separate BWR from PWR
BranchProbability 02 14 0.041667
BranchProbability 02 15 0.041667
BranchProbability 02 16 0.041666
BranchProbability 02 17 0.041667
BranchProbability 02 18 0.041667
BranchProbability 02 19 0.041666
```

```
BranchProbability 02 20 0.041667
BranchProbability 02 21 0.041667
BranchProbability 02 22 0.041666
BranchProbability 02 23 0.041667
BranchProbability 02 24 0.041667

BranchProbability 03 1 0.50 // Discovery
BranchProbability 03 2 0.17
BranchProbability 03 3 0.33
BranchProbability 04 1 0.01 // Accident Severity
BranchProbability 04 2 0.33
BranchProbability 04 3 0.66
BranchProbability 05 1 1/3
BranchProbability 05 2 1/3
BranchProbability 05 3 1/3

BranchProbability 07 1 1

BranchProbability 10 1 0.50 // Sponsorship of attack
BranchProbability 10 2 0.50

TableProbabilityType T1 ABS // Adversary numbers - minimal notice
T1 3 5 7
T1p 25 50 25

TableProbabilityType T2 ABS // Adversary numbers - notice given
T2 5 7 8
T2p 25 50 25

TableProbabilityType T3 ABS // Response force numbers - minimal accident
T3 2 4 6 8
T3p 10 20 30 40

TableProbabilityType T4 ABS // Response force numbers - moderate accident
T4 2 4 6 8
T4p 13 24 40 23

TableProbabilityType T5 ABS // Response force numbers - severe accident
T5 2 4 6 8
T5p 23 40 24 13

//
================================================================================================
==========
// ======================================== initial values
==========================================
//
================================================================================================
==========
INIT  V103      0.0      // placeholder value for accident severities (routine)
INIT  V104      0.0      // placeholder value for accident severities
INIT  V105      0.0      // placeholder value for accident severities

INIT  V201      0.0      // placeholder value for SNF inventory
INIT  V202      0.0      // placeholder value for SNF inventory
INIT  V203      0.0      // placeholder value for SNF inventory
INIT  V204      0.0      // placeholder value for SNF inventory
INIT  V205      0.0      // placeholder value for SNF inventory
INIT  V206      0.0      // placeholder value for SNF inventory
INIT  V207      0.0      // placeholder value for SNF inventory
INIT  V208      0.0      // placeholder value for SNF inventory
INIT  V209      0.0      // placeholder value for SNF inventory
INIT  V210      0.0      // placeholder value for SNF inventory
INIT  V211      0.0      // placeholder value for SNF inventory
INIT  V212      0.0      // placeholder value for SNF inventory
INIT  V213      0.0      // placeholder value for SNF inventory
```

```
INIT  V214      0.0      // placeholder value for SNF inventory
INIT  V215      0.0      // placeholder value for SNF inventory
INIT  V216      0.0      // placeholder value for SNF inventory
INIT  V217      0.0      // placeholder value for SNF inventory
INIT  V218      0.0      // placeholder value for SNF inventory
INIT  V219      0.0      // placeholder value for SNF inventory
INIT  V220      0.0      // placeholder value for SNF inventory
INIT  V221      0.0      // placeholder value for SNF inventory
INIT  V222      0.0      // placeholder value for SNF inventory
INIT  V223      0.0      // placeholder value for SNF inventory
INIT  V224      0.0      // placeholder value for SNF inventory
INIT  V225      0.0      // placeholder value for SNF inventory
INIT  V226      0.0      // placeholder value for SNF inventory
INIT  V227      0.0      // placeholder value for SNF inventory
INIT  V228      0.0      // placeholder value for SNF inventory
INIT  V229      0.0      // placeholder value for SNF inventory
INIT  V230      0.0      // placeholder value for SNF inventory
INIT  V231      0.0      // placeholder value for SNF inventory
INIT  V232      0.0      // placeholder value for SNF inventory

INIT  V111      1        // placeholder for evacuation time (d)

INIT  V101      07       // initial stopcode

// =========================
// STAGE Initial Variables
// =========================

INIT  V1011     0.5      // LLE time for arrival (Immediate)
INIT  V1012     7        // Number of adversaries
INIT  V1013     8        // Number of response forces
INIT  V1014     0        // Additional delay at cask from wreckage
INIT  V1015     0        // Extra attackers due to sponsorship

//
================================================================================================
==========
// ======================================== branching input
==========================================
//
================================================================================================
==========

// ================================== Advanced Notice branches
================================
01 1  V101    03         // Minimal local LE warning
01 1  V111    1          // Default evacuation time
01 1  V1011   1.5        // STAGE time for outside LE arrival
01 1  V1012   T1         // Attacker distribution

01 2  V101    03         // Minimal local LE warning
01 2  V111    1          // Default evacuation time
01 2  V1011   2.5        // STAGE time for outside LE arrival
01 2  V1012   T1         // Attacker distribution

01 3  V101    03         // Minimal local LE warning
01 3  V111    1          // Default evacuation time
01 3  V1011   3.5        // STAGE time for outside LE arrival
01 3  V1012   T1         // Attacker distribution

01 4  V101    03         // Heightened local LE warning
01 4  V111    0.5        // Shortened evacuation time
01 4  V1011   0.5        // STAGE time for outside LE arrival
01 4  V1012   T2         // Attacker distribution assuming possibility of LE insider/leak

01 5  V101    03         // Heightened local LE warning
```

```
01 5  V111    0.5        // Shortened evacuation time
01 5  V1011   1.5        // STAGE time for outside LE arrival
01 5  V1012   T2         // Attacker distribution assuming possibility of LE insider/leak

01 6  V101    03         // Heightened local LE warning
01 6  V111    0.5        // Shortened evacuation time
01 6  V1011   2.5        // STAGE time for outside LE arrival
01 6  V1012   T2         // Attacker distribution assuming possibility of LE insider/leak

// ================================= nuclide inventory branches
================================
02 1  V101    10         // PWR 60GWd-5y
02 1  V201    12468.32   // Am241
02 1  V202    71.35784   // Am242
02 1  V203    71.68865   // Am242m
02 1  V204    670.2486   // Am243
02 1  V205    114214.1   // Ce144
02 1  V206    396.8951   // Cm243
02 1  V207    147120     // Cm244
02 1  V208    11904.65   // Co60
02 1  V209    740886.5   // Cs134
02 1  V210    1840670    // Cs137
02 1  V211    86309.19   // Eu154
02 1  V212    39121.3    // Eu155
02 1  V213    130144.9   // Kr85
02 1  V214    89429.19   // Pu238
02 1  V215    2536.411   // Pu239
02 1  V216    5443.914   // Pu240
02 1  V217    1146357    // Pu241
02 1  V218    54.557169  // Pu242
02 1  V219    221448.6   // Ru106
02 1  V220    39970.38   // Sb125
02 1  V221    1259935    // Sr90
02 1  V222    9787.459   // Te125m
02 1  V223    11.73016   // U234
02 1  V224    1260259    // Y90
02 1  V225    1743114    // Ba137m
02 1  V226    427.7643   // Cm242
02 1  V227    670.2486   // Np239
02 1  V228    114220.5   // Pr144
02 1  V229    1090.573   // Pr144m
02 1  V230    221448.6   // Rh106
02 1  V231    0.4853947  // Te127
02 1  V232    0.495555   // Te127m

02 2  V101    10         // PWR 60GWd-10y
02 2  V201    20484.97   // Am241
02 2  V202    69.62595   // Am242
02 2  V203    69.94378   // Am242m
02 2  V204    669.9243   // Am243
02 2  V205    1347.308   // Ce144
02 2  V206    352.3654   // Cm243
02 2  V207    121511.4   // Cm244
02 2  V208    6170.919   // Co60
02 2  V209    138493     // Cs134
02 2  V210    1640497    // Cs137
02 2  V211    57701.19   // Eu154
02 2  V212    18877.62   // Eu155
02 2  V213    94313.51   // Kr85
02 2  V214    85965.41   // Pu238
02 2  V215    2536.216   // Pu239
02 2  V216    5511.697   // Pu240
02 2  V217    899610.8   // Pu241
02 2  V218    54.55654   // Pu242
02 2  V219    7371.892   // Ru106
02 2  V220    11388.97   // Sb125
```

```
02 2  V221    1117168    // Sr90
02 2  V222    2788.8     // Te125m
02 2  V223    12.96714   // U234
02 2  V224    1117427    // Y90
02 2  V225    1553514    // Ba137m
02 2  V226    57.87373   // Cm242
02 2  V227    669.9243   // Np239
02 2  V228    1347.308   // Pr144
02 2  V229    12.864     // Pr144m
02 2  V230    7371.892   // Rh106
02 2  V231    0.00000442 // Te127
02 2  V232    0.00000452 // Te127m

02 3  V101    10         // PWR 60GWd-25y
02 3  V201    35148.32   // Am241
02 3  V202    64.68      // Am242
02 3  V203    64.97514   // Am242m
02 3  V204    668.9514   // Am243
02 3  V205    0.002211   // Ce144
02 3  V206    246.5578   // Cm243
02 3  V207    68464.86   // Cm244
02 3  V208    859.5892   // Co60
02 3  V209    904.5405   // Cs134
02 3  V210    1161341    // Cs137
02 3  V211    17239.78   // Eu154
02 3  V212    2121.081   // Eu155
02 3  V213    35896.22   // Kr85
02 3  V214    76371.89   // Pu238
02 3  V215    2535.503   // Pu239
02 3  V216    5649.341   // Pu240
02 3  V217    434802.2   // Pu241
02 3  V218    54.55589   // Pu242
02 3  V219    0.271933   // Ru106
02 3  V220    263.4486   // Sb125
02 3  V221    778702.7   // Sr90
02 3  V222    64.51135   // Te125m
02 3  V223    16.39784   // U234
02 3  V224    778897.3   // Y90
02 3  V225    1099784    // Ba137m
02 3  V226    53.49106   // Cm242
02 3  V227    668.9514   // Np239
02 3  V228    0.002211   // Pr144
02 3  V229    0.0000211  // Pr144m
02 3  V230    0.271933   // Rh106
02 3  V231    3.35E-21   // Te127
02 3  V232    3.42E-21   // Te127m

02 4  V101    10         // PWR 60GWd-50y
02 4  V201    43619.03   // Am241
02 4  V202    57.20497   // Am242
02 4  V203    57.46768   // Am242m
02 4  V204    667.3946   // Am243
02 4  V205    5.05E-13   // Ce144
02 4  V206    135.9827   // Cm243
02 4  V207    26313.08   // Cm244
02 4  V208    32.17232   // Co60
02 4  V209    0.206432   // Cs134
02 4  V210    653059.5   // Cs137
02 4  V211    2302.119   // Eu154
02 4  V212    55.49319   // Eu155
02 4  V213    7175.351   // Kr85
02 4  V214    62693.84   // Pu238
02 4  V215    2534.335   // Pu239
02 4  V216    5750.595   // Pu240
02 4  V217    129437.8   // Pu241
02 4  V218    54.55459   // Pu242
```

```
02 4  V219    1.11E-08   // Ru106
02 4  V220    0.49477    // Sb125
02 4  V221    426720     // Sr90
02 4  V222    0.121155   // Te125m
02 4  V223    21.28541   // U234
02 4  V224    426830.3   // Y90
02 4  V225    618415.1   // Ba137m
02 4  V226    47.30854   // Cm242
02 4  V227    667.3946   // Np239
02 4  V228    5.05E-13   // Pr144
02 4  V229    4.82E-15   // Pr144m
02 4  V230    1.11E-08   // Rh106
02 4  V231    0          // Te127
02 4  V232    0          // Te127m

02 5  V101    10         // PWR 50GWd-5y
02 5  V201    12151.78   // Am241
02 5  V202    74.29622   // Am242
02 5  V203    74.64      // Am242m
02 5  V204    424.1189   // Am243
02 5  V205    117853     // Ce144
02 5  V206    275.5005   // Cm243
02 5  V207    70378.38   // Cm244
02 5  V208    9718.054   // Co60
02 5  V209    552136.2   // Cs134
02 5  V210    1549686    // Cs137
02 5  V211    72181.62   // Eu154
02 5  V212    31724.76   // Eu155
02 5  V213    117645.4   // Kr85
02 5  V214    64120.22   // Pu238
02 5  V215    2621.903   // Pu239
02 5  V216    4966.249   // Pu240
02 5  V217    1105168    // Pu241
02 5  V218    37.05016   // Pu242
02 5  V219    182588.1   // Ru106
02 5  V220    34038.49   // Sb125
02 5  V221    1125211    // Sr90
02 5  V222    8335.135   // Te125m
02 5  V223    13.88303   // U234
02 5  V224    1125470    // Y90
02 5  V225    1467503    // Ba137m
02 5  V226    369.4054   // Cm242
02 5  V227    424.1189   // Np239
02 5  V228    117859.5   // Pr144
02 5  V229    1125.276   // Pr144m
02 5  V230    182588.1   // Rh106
02 5  V231    0.492564   // Te127
02 5  V232    0.502871   // Te127m

02 6  V101    10         // PWR 50GWd-10y
02 6  V201    19879.78   // Am241
02 6  V202    72.49297   // Am242
02 6  V203    72.83027   // Am242m
02 6  V204    423.9178   // Am243
02 6  V205    1390.184   // Ce144
02 6  V206    244.5859   // Cm243
02 6  V207    58128.65   // Cm244
02 6  V208    5037.665   // Co60
02 6  V209    103206.5   // Cs134
02 6  V210    1381103    // Cs137
02 6  V211    48252.97   // Eu154
02 6  V212    15308.76   // Eu155
02 6  V213    85258.38   // Kr85
02 6  V214    61641.08   // Pu238
02 6  V215    2621.643   // Pu239
02 6  V216    4997.449   // Pu240
```

```
02 6  V217    867308.1   // Pu241
02 6  V218    37.05016   // Pu242
02 6  V219    6078.097   // Ru106
02 6  V220    9698.595   // Sb125
02 6  V221    997621.6   // Sr90
02 6  V222    2374.897   // Te125m
02 6  V223    14.76973   // U234
02 6  V224    997881.1   // Y90
02 6  V225    1307935    // Ba137m
02 6  V226    60.22573   // Cm242
02 6  V227    423.9178   // Np239
02 6  V228    1390.249   // Pr144
02 6  V229    13.2733    // Pr144m
02 6  V230    6078.097   // Rh106
02 6  V231    4.49E-06   // Te127
02 6  V232    4.58E-06   // Te127m

02 7  V101    10         // PWR 50GWd-25y
02 7  V201    34013.84   // Am241
02 7  V202    67.3427    // Am242
02 7  V203    67.65405   // Am242m
02 7  V204    423.3211   // Am243
02 7  V205    0.002282   // Ce144
02 7  V206    171.1459   // Cm243
02 7  V207    32750.92   // Cm244
02 7  V208    701.7081   // Co60
02 7  V209    674.0757   // Cs134
02 7  V210    977708.1   // Cs137
02 7  V211    14417.51   // Eu154
02 7  V212    1720.022   // Eu155
02 7  V213    32449.95   // Kr85
02 7  V214    54760.86   // Pu238
02 7  V215    2620.8     // Pu239
02 7  V216    5059.524   // Pu240
02 7  V217    419189.2   // Pu241
02 7  V218    37.04951   // Pu242
02 7  V219    0.224212   // Ru106
02 7  V220    224.3546   // Sb125
02 7  V221    695416.2   // Sr90
02 7  V222    54.9373    // Te125m
02 7  V223    17.23005   // U234
02 7  V224    695610.8   // Y90
02 7  V225    925881.1   // Ba137m
02 7  V226    55.69492   // Cm242
02 7  V227    423.3211   // Np239
02 7  V228    0.002282   // Pr144
02 7  V229    2.18E-05   // Pr144m
02 7  V230    0.224212   // Rh106
02 7  V231    3.4E-21    // Te127
02 7  V232    3.47E-21   // Te127m

02 8  V101    10         // PWR 50GWd-50y
02 8  V201    42174.49   // Am241
02 8  V202    59.56216   // Am242
02 8  V203    59.83589   // Am242m
02 8  V204    422.3286   // Am243
02 8  V205    5.21E-13   // Ce144
02 8  V206    94.39135   // Cm243
02 8  V207    12587.68   // Cm244
02 8  V208    26.26443   // Co60
02 8  V209    0.153834   // Cs134
02 8  V210    549781.6   // Cs137
02 8  V211    48252.97   // Eu154
02 8  V212    45.00065   // Eu155
02 8  V213    6486.227   // Kr85
02 8  V214    44957.84   // Pu238
```

```
02 8  V215    2619.308   // Pu239
02 8  V216    5101.751   // Pu240
02 8  V217    124780.5   // Pu241
02 8  V218    37.04886   // Pu242
02 8  V219    9.17E-09   // Ru106
02 8  V220    0.421343   // Sb125
02 8  V221    381074.6   // Sr90
02 8  V222    0.103174   // Te125m
02 8  V223    20.73405   // U234
02 8  V224    381171.9   // Y90
02 8  V225    520644.3   // Ba137m
02 8  V226    49.25773   // Cm242
02 8  V227    422.3286   // Np239
02 8  V228    5.21E-13   // Pr144
02 8  V229    4.98E-15   // Pr144m
02 8  V230    9.17E-09   // Rh106
02 8  V231    0          // Te127
02 8  V232    0          // Te127m

02 9  V101    10         // PWR 40GWd-5y
02 9  V201    10869.41   // Am241
02 9  V202    67.00541   // Am242
02 9  V203    67.31027   // Am242m
02 9  V204    222.6357   // Am243
02 9  V205    119344.9   // Ce144
02 9  V206    149.1178   // Cm243
02 9  V207    26434.38   // Cm244
02 9  V208    7624.865   // Co60
02 9  V209    378259.5   // Cs134
02 9  V210    1252476    // Cs137
02 9  V211    54531.24   // Eu154
02 9  V212    23178.16   // Eu155
02 9  V213    101798.9   // Kr85
02 9  V214    39586.38   // Pu238
02 9  V215    2697.341   // Pu239
02 9  V216    4248.389   // Pu240
02 9  V217    988540.5   // Pu241
02 9  V218    22.00086   // Pu242
02 9  V219    143597.8   // Ru106
02 9  V220    27867.89   // Sb125
02 9  V221    961686.5   // Sr90
02 9  V222    6823.784   // Te125m
02 9  V223    16.27784   // U234
02 9  V224    961945.9   // Y90
02 9  V225    1186054    // Ba137m
02 9  V226    270.8562   // Cm242
02 9  V227    222.6357   // Np239
02 9  V228    119351.4   // Pr144
02 9  V229    1139.546   // Pr144m
02 9  V230    143597.8   // Rh106
02 9  V231    0.496839   // Te127
02 9  V232    0.507243   // Te127m

02 10 V101    10         // PWR 40GWd-10y
02 10 V201    17782.05   // Am241
02 10 V202    65.3773    // Am242
02 10 V203    65.67568   // Am242m
02 10 V204    222.5319   // Am243
02 10 V205    1407.762   // Ce144
02 10 V206    132.3892   // Cm243
02 10 V207    21832.86   // Cm244
02 10 V208    3952.605   // Co60
02 10 V209    70702.7    // Cs134
02 10 V210    1116259    // Cs137
02 10 V211    36456      // Eu154
02 10 V212    11184.65   // Eu155
```

```
02 10 V213    73770.81   // Kr85
02 10 V214    38056.86   // Pu238
02 10 V215    2696.951   // Pu239
02 10 V216    4258.768   // Pu240
02 10 V217    775783.8   // Pu241
02 10 V218    22.00086   // Pu242
02 10 V219    4780.281   // Ru106
02 10 V220    7940.108   // Sb125
02 10 V221    852648.6   // Sr90
02 10 V222    1944.389   // Te125m
02 10 V223    16.8253    // U234
02 10 V224    852908.1   // Y90
02 10 V225    1057103    // Ba137m
02 10 V226    54.2867    // Cm242
02 10 V227    222.5319   // Np239
02 10 V228    1407.827   // Pr144
02 10 V229    13.4413    // Pr144m
02 10 V230    4780.281   // Rh106
02 10 V231    0          // Te127
02 10 V232    4.62E-06   // Te127m

02 11 V101    10         // PWR 40GWd-25y
02 11 V201    30424.22   // Am241
02 11 V202    60.73362   // Am242
02 11 V203    61.01254   // Am242m
02 11 V204    222.2205   // Am243
02 11 V205    0.002311   // Ce144
02 11 V206    92.63351   // Cm243
02 11 V207    12300.97   // Cm244
02 11 V208    550.5665   // Co60
02 11 V209    461.7989   // Cs134
02 11 V210    790183.8   // Cs137
02 11 V211    10892.11   // Eu154
02 11 V212    1256.692   // Eu155
02 11 V213    28078.05   // Kr85
02 11 V214    22810.16   // Pu238
02 11 V215    2695.914   // Pu239
02 11 V216    4278.357   // Pu240
02 11 V217    374951.4   // Pu241
02 11 V218    22.00086   // Pu242
02 11 V219    0.176335   // Ru106
02 11 V220    183.6843   // Sb125
02 11 V221    594356.8   // Sr90
02 11 V222    44.97795   // Te125m
02 11 V223    18.34378   // U234
02 11 V224    594505.9   // Y90
02 11 V225    748345.9   // Ba137m
02 11 V226    50.22616   // Cm242
02 11 V227    222.2205   // Np239
02 11 V228    0.002311   // Pr144
02 11 V229    2.21E-05   // Pr144m
02 11 V230    0.176335   // Rh106
02 11 V231    3.43E-21   // Te127
02 11 V232    3.5E-21    // Te127m

02 12 V101    10         // PWR 40GWd-25y
02 12 V201    37724.11   // Am241
02 12 V202    53.71395   // Am242
02 12 V203    53.96108   // Am242m
02 12 V204    221.6951   // Am243
02 12 V205    5.28E-13   // Ce144
02 12 V206    51.09016   // Cm243
02 12 V207    4727.741   // Cm244
02 12 V208    20.60692   // Co60
02 12 V209    0.105386   // Cs134
02 12 V210    444343.8   // Cs137
```

```
02 12 V211    1454.53    // Eu154
02 12 V212    32.87805   // Eu155
02 12 V213    5612.432   // Kr85
02 12 V214    27760.86   // Pu238
02 12 V215    2694.227   // Pu239
02 12 V216    4287.957   // Pu240
02 12 V217    111606.5   // Pu241
02 12 V218    22.00022   // Pu242
02 12 V219    7.21E-09   // Ru106
02 12 V220    0.344958   // Sb125
02 12 V221    325699.5   // Sr90
02 12 V222    0.084467   // Te125m
02 12 V223    20.50703   // U234
02 12 V224    325783.8   // Y90
02 12 V225    420791.4   // Ba137m
02 12 V226    44.42141   // Cm242
02 12 V227    221.6951   // Np239
02 12 V228    5.28E-13   // Pr144
02 12 V229    5.04E-15   // Pr144m
02 12 V230    7.21E-09   // Rh106
02 12 V231    0          // Te127
02 12 V232    0          // Te127m

02 13 V101    10         // BWR 60GWd-5y
02 13 V201    12579.08   // Am241
02 13 V202    69.25135   // Am242
02 13 V203    69.57038   // Am242m
02 13 V204    554.9946   // Am243
02 13 V205    78638.05   // Ce144
02 13 V206    345.1957   // Cm243
02 13 V207    93449.62   // Cm244
02 13 V208    22130.92   // Co60
02 13 V209    493114.6   // Cs134
02 13 V210    1433092    // Cs137
02 13 V211    70146.59   // Eu154
02 13 V212    32502.81   // Eu155
02 13 V213    97161.3    // Kr85
02 13 V214    64903.03   // Pu238
02 13 V215    2757.968   // Pu239
02 13 V216    6351.168   // Pu240
02 13 V217    1097355    // Pu241
02 13 V218    39.08995   // Pu242
02 13 V219    159260.5   // Ru106
02 13 V220    29156.54   // Sb125
02 13 V221    963152.4   // Sr90
02 13 V222    7139.6     // Te125m
02 13 V223    10.50203   // U234
02 13 V224    963391.4   // Y90
02 13 V225    1357059    // Ba137m
02 13 V226    404.1805   // Cm242
02 13 V227    554.9946   // Np239
02 13 V228    78640.86   // Pr144
02 13 V229    750.8378   // Pr144m
02 13 V230    159260.5   // Rh106
02 13 V231    0          // Te127
02 13 V232    0.44089    // Te127m

02 14 V101    10         // BWR 60GWd-10y
02 14 V201    20247.68   // Am241
02 14 V202    67.57189   // Am242
02 14 V203    67.88249   // Am242m
02 14 V204    554.7276   // Am243
02 14 V205    927.5957   // Ce144
02 14 V206    306.4627   // Cm243
02 14 V207    77183.46   // Cm244
02 14 V208    11472.04   // Co60
```

```
02 14 V209    92176.32   // Cs134
02 14 V210    1277176    // Cs137
02 14 V211    46895.57   // Eu154
02 14 V212    15684.32   // Eu155
02 14 V213    70412.22   // Kr85
02 14 V214    62394.38   // Pu238
02 14 V215    2757.686   // Pu239
02 14 V216    6392.768   // Pu240
02 14 V217    861162.2   // Pu241
02 14 V218    39.08995   // Pu242
02 14 V219    5301.33    // Ru106
02 14 V220    8307.632   // Sb125
02 14 V221    853980.5   // Sr90
02 14 V222    2034.324   // Te125m
02 14 V223    11.39981   // U234
02 14 V224    854191.4   // Y90
02 14 V225    1209478    // Ba137m
02 14 V226    56.16      // Cm242
02 14 V227    554.7276   // Np239
02 14 V228    927.6378   // Pr144
02 14 V229    8.856724   // Pr144m
02 14 V230    5301.33    // Rh106
02 14 V231    3.94E-06   // Te127
02 14 V232    4.02E-06   // Te127m

02 15 V101    10         // BWR 60GWd-25y
02 15 V201    34269.41   // Am241
02 15 V202    62.77103   // Am242
02 15 V203    63.06054   // Am242m
02 15 V204    553.9546   // Am243
02 15 V205    0.001522   // Ce144
02 15 V206    214.4508   // Cm243
02 15 V207    43486.05   // Cm244
02 15 V208    1597.946   // Co60
02 15 V209    602.0335   // Cs134
02 15 V210    904139.5   // Cs137
02 15 V211    14011.47   // Eu154
02 15 V212    1762.238   // Eu155
02 15 V213    26799.68   // Kr85
02 15 V214    55427.78   // Pu238
02 15 V215    2756.843   // Pu239
02 15 V216    6475.546   // Pu240
02 15 V217    416210.8   // Pu241
02 15 V218    39.08854   // Pu242
02 15 V219    0.195562   // Ru106
02 15 V220    192.1751   // Sb125
02 15 V221    595259.5   // Sr90
02 15 V222    47.05859   // Te125m
02 15 V223    13.88976   // U234
02 15 V224    595414.1   // Y90
02 15 V225    856215.1   // Ba137m
02 15 V226    51.91146   // Cm242
02 15 V227    553.9546   // Np239
02 15 V228    0.001522   // Pr144
02 15 V229    1.45E-05   // Pr144m
02 15 V230    0.195562   // Rh106
02 15 V231    2.98E-21   // Te127
02 15 V232    3.04E-21   // Te127m

02 16 V101    10         // BWR 60GWd-50y
02 16 V201    42353.3    // Am241
02 16 V202    55.51632   // Am242
02 16 V203    55.77211   // Am242m
02 16 V204    552.6476   // Am243
02 16 V205    3.48E-13   // Ce144
02 16 V206    118.2691   // Cm243
```

```
02 16 V207    16713.08   // Cm244
02 16 V208    59.80984   // Co60
02 16 V209    0.13739    // Cs134
02 16 V210    508405.4   // Cs137
02 16 V211    1871.016   // Eu154
02 16 V212    46.10432   // Eu155
02 16 V213    5356.843   // Kr85
02 16 V214    45505.62   // Pu238
02 16 V215    2755.297   // Pu239
02 16 V216    6532.324   // Pu240
02 16 V217    123896.3   // Pu241
02 16 V218    39.08854   // Pu242
02 16 V219    7.99E-09   // Ru106
02 16 V220    0.360908   // Sb125
02 16 V221    326194.6   // Sr90
02 16 V222    0.088378   // Te125m
02 16 V223    17.43686   // U234
02 16 V224    326278.9   // Y90
02 16 V225    481449.7   // Ba137m
02 16 V226    45.91178   // Cm242
02 16 V227    552.6476   // Np239
02 16 V228    3.48E-13   // Pr144
02 16 V229    3.32E-15   // Pr144m
02 16 V230    7.99E-09   // Rh106
02 16 V231    0          // Te127
02 16 V232    0          // Te127m

02 17 V101    10         // BWR 50GWd-5y
02 17 V201    11597.41   // Am241
02 17 V202    63.99654   // Am242
02 17 V203    64.29027   // Am242m
02 17 V204    331.5914   // Am243
02 17 V205    81728.54   // Ce144
02 17 V206    224.4714   // Cm243
02 17 V207    43931.57   // Cm244
02 17 V208    18790.27   // Co60
02 17 V209    372629.2   // Cs134
02 17 V210    1209689    // Cs137
02 17 V211    57665.19   // Eu154
02 17 V212    26033.73   // Eu155
02 17 V213    88384.54   // Kr85
02 17 V214    45401.62   // Pu238
02 17 V215    2837.232   // Pu239
02 17 V216    5631.741   // Pu240
02 17 V217    1011147    // Pu241
02 17 V218    26.68443   // Pu242
02 17 V219    135701.7   // Ru106
02 17 V220    25436.43   // Sb125
02 17 V221    860276.8   // Sr90
02 17 V222    6228.757   // Te125m
02 17 V223    11.94187   // U234
02 17 V224    860487.6   // Y90
02 17 V225    1145560    // Ba137m
02 17 V226    323.96     // Cm242
02 17 V227    331.5914   // Np239
02 17 V228    81731.35   // Pr144
02 17 V229    780.3373   // Pr144m
02 17 V230    135701.7   // Rh106
02 17 V231    0.432977   // Te127
02 17 V232    0.442042   // Te127m

02 18 V101    10         // BWR 50GWd-10y
02 18 V201    18663.78   // Am241
02 18 V202    62.44357   // Am242
02 18 V203    62.73027   // Am242m
02 18 V204    331.4368   // Am243
```

```
02 18 V205    964.0659   // Ce144
02 18 V206    199.2865   // Cm243
02 18 V207    36283.35   // Cm244
02 18 V208    9740.303   // Co60
02 18 V209    69653.3    // Cs134
02 18 V210    1078115    // Cs137
02 18 V211    38550.27   // Eu154
02 18 V212    12562.64   // Eu155
02 18 V213    64051.35   // Kr85
02 18 V214    43646.27   // Pu238
02 18 V215    2836.951   // Pu239
02 18 V216    5650.011   // Pu240
02 18 V217    793520     // Pu241
02 18 V218    26.68443   // Pu242
02 18 V219    4517.395   // Ru106
02 18 V220    7247.676   // Sb125
02 18 V221    762769.7   // Sr90
02 18 V222    1774.746   // Te125m
02 18 V223    12.56966   // U234
02 18 V224    762966.5   // Y90
02 18 V225    1020971    // Ba137m
02 18 V226    51.87773   // Cm242
02 18 V227    331.4368   // Np239
02 18 V228    964.0941   // Pr144
02 18 V229    9.204843   // Pr144m
02 18 V230    4517.395   // Rh106
02 18 V231    3.95E-06   // Te127
02 18 V232    4.03E-06   // Te127m

02 19 V101    10         // BWR 50GWd-25y
02 19 V201    31583.68   // Am241
02 19 V202    58.0067    // Am242
02 19 V203    58.27373   // Am242m
02 19 V204    330.973    // Am243
02 19 V205    0.001582   // Ce144
02 19 V206    139.4457   // Cm243
02 19 V207    20443.03   // Cm244
02 19 V208    1356.736   // Co60
02 19 V209    454.9297   // Cs134
02 19 V210    763219.5   // Cs137
02 19 V211    11518.28   // Eu154
02 19 V212    1411.589   // Eu155
02 19 V213    24378.16   // Kr85
02 19 V214    38775.14   // Pu238
02 19 V215    2835.968   // Pu239
02 19 V216    5684.724   // Pu240
02 19 V217    383521.1   // Pu241
02 19 V218    26.68443   // Pu242
02 19 V219    0.166639   // Ru106
02 19 V220    167.6508   // Sb125
02 19 V221    531678.9   // Sr90
02 19 V222    41.0547    // Te125m
02 19 V223    14.31124   // U234
02 19 V224    531819.5   // Y90
02 19 V225    722771.9   // Ba137m
02 19 V226    47.97211   // Cm242
02 19 V227    330.973    // Np239
02 19 V228    0.001582   // Pr144
02 19 V229    1.51E-05   // Pr144m
02 19 V230    0.166639   // Rh106
02 19 V231    2.99E-21   // Te127
02 19 V232    3.05E-21   // Te127m

02 20 V101    10         // BWR 50GWd-50y
02 20 V201    39032.32   // Am241
02 20 V202    51.30292   // Am242
```

```
02 20 V203    51.53903   // Am242m
02 20 V204    330.2      // Am243
02 20 V205    3.61E-13   // Ce144
02 20 V206    76.90519   // Cm243
02 20 V207    7857.059   // Cm244
02 20 V208    50.78151   // Co60
02 20 V209    0.103819   // Cs134
02 20 V210    429168.6   // Cs137
02 20 V211    1538.076   // Eu154
02 20 V212    36.92843   // Eu155
02 20 V213    4872.962   // Kr85
02 20 V214    31835.24   // Pu238
02 20 V215    2834.141   // Pu239
02 20 V216    5704.4     // Pu240
02 20 V217    114156.9   // Pu241
02 20 V218    26.68303   // Pu242
02 20 V219    6.81E-09   // Ru106
02 20 V220    0.314867   // Sb125
02 20 V221    291354.6   // Sr90
02 20 V222    0.077101   // Te125m
02 20 V223    16.79319   // U234
02 20 V224    291424.9   // Y90
02 20 V225    406415.1   // Ba137m
02 20 V226    42.42778   // Cm242
02 20 V227    330.2      // Np239
02 20 V228    3.61E-13   // Pr144
02 20 V229    3.45E-15   // Pr144m
02 20 V230    6.81E-09   // Rh106
02 20 V231    0          // Te127
02 20 V232    0          // Te127m

02 21 V101    10         // BWR 40GWd-5y
02 21 V201    9753.654   // Am241
02 21 V202    50.98811   // Am242
02 21 V203    51.22281   // Am242m
02 21 V204    164.067    // Am243
02 21 V205    84178.16   // Ce144
02 21 V206    115.7295   // Cm243
02 21 V207    16090.49   // Cm244
02 21 V208    15338.59   // Co60
02 21 V209    260126.5   // Cs134
02 21 V210    980059.5   // Cs137
02 21 V211    42541.62   // Eu154
02 21 V212    18769.19   // Eu155
02 21 V213    77083.68   // Kr85
02 21 V214    27538.92   // Pu238
02 21 V215    2878.832   // Pu239
02 21 V216    4650.205   // Pu240
02 21 V217    860853     // Pu241
02 21 V218    15.97665   // Pu242
02 21 V219    110664.4   // Ru106
02 21 V220    21311.57   // Sb125
02 21 V221    736797.8   // Sr90
02 21 V222    5218.551   // Te125m
02 21 V223    13.57411   // U234
02 21 V224    736980.5   // Y90
02 21 V225    928101.6   // Ba137m
02 21 V226    220.733    // Cm242
02 21 V227    164.067    // Np239
02 21 V228    84180.97   // Pr144
02 21 V229    803.7232   // Pr144m
02 21 V230    110665.8   // Rh106
02 21 V231    0.429871   // Te127
02 21 V232    0.43888    // Te127m

02 22 V101    10         // BWR 40GWd-10y
```

```
02 22 V201    15770.05   // Am241
02 22 V202    49.75135   // Am242
02 22 V203    49.98043   // Am242m
02 22 V204    163.9968   // Am243
02 22 V205    992.947    // Ce144
02 22 V206    102.7436   // Cm243
02 22 V207    13289.94   // Cm244
02 22 V208    7951.222   // Co60
02 22 V209    48624.22   // Cs134
02 22 V210    873473.5   // Cs137
02 22 V211    28439.78   // Eu154
02 22 V212    9057.276   // Eu155
02 22 V213    55862.05   // Kr85
02 22 V214    26475.03   // Pu238
02 22 V215    2878.411   // Pu239
02 22 V216    4655.405   // Pu240
02 22 V217    675564.3   // Pu241
02 22 V218    15.97665   // Pu242
02 22 V219    3683.849   // Ru106
02 22 V220    6072.335   // Sb125
02 22 V221    653274.6   // Sr90
02 22 V222    1486.919   // Te125m
02 22 V223    13.95497   // U234
02 22 V224    653443.2   // Y90
02 22 V225    827165.4   // Ba137m
02 22 V226    41.31751   // Cm242
02 22 V227    163.9968   // Np239
02 22 V228    992.9751   // Pr144
02 22 V229    9.480584   // Pr144m
02 22 V230    3683.849   // Rh106
02 22 V231    3.92E-06   // Te127
02 22 V232    4E-06      // Te127m

02 23 V101    10         // BWR 40GWd-25y
02 23 V201    26772.97   // Am241
02 23 V202    46.21676   // Am242
02 23 V203    46.43038   // Am242m
02 23 V204    163.7578   // Am243
02 23 V205    0.00163    // Ce144
02 23 V206    71.89351   // Cm243
02 23 V207    7487.859   // Cm244
02 23 V208    1107.544   // Co60
02 23 V209    317.5795   // Cs134
02 23 V210    618350.3   // Cs137
02 23 V211    8497.362   // Eu154
02 23 V212    1017.668   // Eu155
02 23 V213    21260.97   // Kr85
02 23 V214    23522.27   // Pu238
02 23 V215    2877.286   // Pu239
02 23 V216    4664.119   // Pu240
02 23 V217    326503.8   // Pu241
02 23 V218    15.97665   // Pu242
02 23 V219    0.135894   // Ru106
02 23 V220    140.4689   // Sb125
02 23 V221    455365.4   // Sr90
02 23 V222    34.39589   // Te125m
02 23 V223    15.01114   // U234
02 23 V224    455491.9   // Y90
02 23 V225    585562.2   // Ba137m
02 23 V226    38.22141   // Cm242
02 23 V227    163.7578   // Np239
02 23 V228    0.00163    // Pr144
02 23 V229    1.56E-05   // Pr144m
02 23 V230    0.135894   // Rh106
02 23 V231    2.97E-21   // Te127
02 23 V232    3.03E-21   // Te127m
```

```
02 24 V101    10         // BWR 40GWd-50y
02 24 V201    33118.38   // Am241
02 24 V202    40.87622   // Am242
02 24 V203    41.06314   // Am242m
02 24 V204    163.3784   // Am243
02 24 V205    3.72E-13   // Ce144
02 24 V206    39.6507    // Cm243
02 24 V207    2877.849   // Cm244
02 24 V208    41.45384   // Co60
02 24 V209    0.072475   // Cs134
02 24 V210    347697.3   // Cs137
02 24 V211    1134.696   // Eu154
02 24 V212    26.624     // Eu155
02 24 V213    4249.805   // Kr85
02 24 V214    19313.08   // Pu238
02 24 V215    2875.459   // Pu239
02 24 V216    4664.541   // Pu240
02 24 V217    97186.59   // Pu241
02 24 V218    15.97665   // Pu242
02 24 V219    5.56E-09   // Ru106
02 24 V220    0.263809   // Sb125
02 24 V221    249543.8   // Sr90
02 24 V222    0.064598   // Te125m
02 24 V223    16.51632   // U234
02 24 V224    249600     // Y90
02 24 V225    329272.4   // Ba137m
02 24 V226    33.80422   // Cm242
02 24 V227    163.3784   // Np239
02 24 V228    3.72E-13   // Pr144
02 24 V229    3.55E-15   // Pr144m
02 24 V230    5.56E-09   // Rh106
02 24 V231    0          // Te127
02 24 V232    0          // Te127m

// ================================== Discovery branches ================================
03 1  V101    04         // No discovery of track damage
03 2  V101    09        // Discovery -reroute
03 3  V101    05        // Discovery -reduced speed


// ================================== accident severity branches
================================
04  1  V101    02         // Minor accident stopcode
04  1  V103    2.52E-6    // Particulate release fraction
04  1  V104    1.125E-5     // Volatile release fraction
04  1  V105    0.072      // Gaseous release fraction
04  1  V1013   T3         // Number of available response forces
04  1  V1014   0         // Additional time needed for adversaries to traverse wreckage

04  2  V101    02         // Moderate accident stopcode
04  2  V103    3.36E-6    // Particulate release fraction
04  2  V104    1.5E-5     // Volatile release fraction
04  2  V105    0.096       // Gaseous release fraction
04  2  V1013   T4         // Number of available response forces
04  2  V1014   20         // Additional time needed for adversaries to traverse wreckage

04  3  V101    02         // Severe accident stopcode
04  3  V103    1.68E-4    // Particulate release fraction
04  3  V104    7.5E-4     // Volatile release fraction
04  3  V105    0.12       // Gaseous release fraction
04  3  V1013   T5         // Number of available response forces
04  3  V1014   40         // Additional time needed for adversaries to traverse wreckage


05 1  V101    02         // Minor accident stopcode
```

```
05 1  V103    2.52E-6    // Particulate release fraction
05 1  V104    1.125E-5   // Volatile release fraction
05 1  V105    0.072      // Gaseous release fraction

05 2  V101    02         // Moderate accident stopcode
05 2  V103    3.36E-6    // Particulate release fraction
05 2  V104    1.5E-5     // Volatile release fraction
05 2  V105    0.096      // Gaseous release fraction

05 3  V101    02         // Severe accident stopcode
05 3  V103    1.68E-4    // Particulate release fraction
05 3  V104    7.5E-4     // Volatile release fraction
05 3  V105    0.12       // Gaseous release fraction

// ================================= TEST ================================

07 1  V101    10          // Dummy, skip to STAGE

// ================================= Sponsorship of Attack
================================
10 1  V1015   0          // No extra attackers from sponsorship
10 2  V1015   1          // Extra support from sponsorship
```

# Appendix C - LS/TS Wrapper for ADAPT and Edit Rules for Case Study 3

This appendix includes the LT/TS wrapper created for ADAPT, as well as the editrules used for the scenario in Case Study 3.

Wrapper file:

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
import os
import sys
import time
import datetime
import shutil
import subprocess
import json
import adaptvars


def setInDict(dataDict, maplist, value):
	first, rest = maplist[0], maplist[1:]
	if isinstance(first[1],dict):
		for x in range(len(dataDict[first[0]])):
			dic = first[1]
			key = list(dic.keys())[0]
			tmpval = dic[key]
			if key in dataDict[first[0]][x] and tmpval ==
dataDict[first[0]][x][key]:
				setInDict(dataDict[first[0]][x], rest, value)
				return
		raise ValueError('correct pathway from \n' + str(dataDict) + '\nnot found
for \n' + str(maplist) + '\nor \n' + str(tmpval))
	if rest:
		try:
			if not isinstance(dataDict[first[0]], dict):
				if not isinstance(dataDict[first[0]], list):
					# if the key is not a dict or list, then make it a
dict
					dataDict[first[0]] = {}
		except KeyError:
			# if key doesn't exist, create one
			dataDict[first[0]] = {}
		setInDict(dataDict[first[0]], rest, value)
	elif str(first) in dataDict:
		print('replacing term ' + str(first) + ' currently at ' +
str(dataDict[first]) + ' with ' + str(value))
		dataDict[first] = value
	else:
```

```
                raise ValueError('correct pathway from \n' + str(dataDict) + '\nnot found
for \n' + str(dataDict[first[0]][x]) + '\nor \n' + str(dataDict[first[0]][x][key]))

        return

def ScribeReplace(location, value, filename):
        with open(str(filename), 'r') as file:
                scribefile = json.load(file)
        setInDict(scribefile, location, value)

        with open(str(filename), 'w') as file:
                json.dump(scribefile, file, indent=4)
        return

def MelcorReplace(adaptvar, value, MELCOR_INPUT):
        with open(MELCOR_INPUT,'r') as file:
                melcorfile = file.read()
        print('replacing dummy value ' + str(adaptvar) + ' with ' + str(value))
        melcorfile = melcorfile.replace(str(adaptvar), str(value))

        with open(MELCOR_INPUT, 'w') as file:
                file.write(melcorfile)
        return

# Set up variables for ADAPT

cwd = os.getcwd()
getenv_adaptrc = os.getenv('ADAPTRC')
getenv_path = os.getenv('PATH')
#server_path = os.path.join(getenv_adaptrc, 'server')
ScribeFile = os.path.join(cwd, 'apiOutput.json')
MELCOR_EXECUTABLE = os.getenv('NCENGINE_EXECUTABLE')
MELCOR_ROOT = cwd
MELCOR_TIME_TEMPLATE = 'TMI.inp.tpl'
MELCOR_TIME_INPUT = 'TMI.inp'
MELCOR_TEMPLATE = 'adapt.gen.tpl'
MELCOR_INPUT = 'adapt.gen'

RST = 'tmi.rst'
MELCOREXE = 'Melcor_RL_NL_CHECKALL_10479.exe'
SCRIBESCENARIO = 'Lone_Pine.ttx'
SCRIBEDIRECTORY = '.'
this_dir = os.getcwd()
stop_word = 'JBWCKY'
for line in getenv_path.split(':'):
        sys.path.insert(0, line)

shutil.copyfile(MELCOR_TEMPLATE, MELCOR_INPUT)


block_time = adaptvars.block_time

# Determine starting scribe time for branch
with open(ScribeFile, 'r') as file:
                sim_elapsed = json.load(file)['SimTime']


# Make ADAPT-related changes to MELCOR and Scribe

for w in adaptvars.Scribe_vars[:]:
        if w[1] == 'Current':
                w[1] = sim_elapsed
        ScribeReplace(w[0], w[1], ScribeFile)

for x in adaptvars.Melcor_vars[:]:
        MelcorReplace(x[0], x[1], MELCOR_INPUT)
```

```
# Run codes
mystopping_code = 0
while mystopping_code == 0:
	# Set end times for Scribe1 and Scribe2
	sim_elapsed = sim_elapsed + block_time
	ScribeReplace(adaptvars.scribe_timepath, sim_elapsed, ScribeFile)
#	MelcorReplace(adaptvars.melcor_timevar, sim_elapsed, MELCOR_TIME_INPUT)


		# Execute first Scribe instance
	ScribeReplace(adaptvars.scribe_stop_condition_path,
adaptvars.scribe_stop_condition, ScribeFile)
	ScribeReplace(adaptvars.scribe_editpath, 'ADAPT', ScribeFile)
	print('started executing Scribe at %s' % (time.asctime()))
	sim1_exec_command = subprocess.run(
		" ".join([
		os.path.join(cwd, "Scribe3D.exe"),
		"-saveFile",
		os.path.join(cwd, "Scribe3D_Data", "StreamingAssets", SCRIBESCENARIO),
		"-adaptFile",
		os.path.join(cwd, "apiOutput.json"),
		"-saveDirectory",
		os.path.join(cwd),
		"-batchmode"
		]),
		env=os.environ,
		stdout=subprocess.PIPE,
		stderr=subprocess.STDOUT
		)
	# Find stopping reason for first branch
	with open(ScribeFile) as output:
		ADV_output = json.load(output)
		ADV_stopReason = ADV_output['StopReason']
		sim_elapsed = ADV_output['StopAtTime']
		if ADV_stopReason.split(':', 1)[0] == 'StoppedAtEvent':
			mystopping_code = ADV_stopReason.split(':', 1)[1].strip()

		elif ADV_stopReason.split(':', 1)[0] == 'Engagment':
			engagement = ADV_output['EntitiesInEngagement']
			mystopping_code = 'Engagement'
		elif ADV_stopReason.split(':', 1)[0] == 'StoppedAtTime':
			print('No adversary stopping condition found during time block')
		else:
			raise ValueError('Unknown stopping reason found for Scribe')


	# Execute MELCOR instance.
	shutil.copyfile(MELCOR_TIME_TEMPLATE, MELCOR_TIME_INPUT)
	MelcorReplace('{EndTime}', float(int(sim_elapsed)), MELCOR_TIME_INPUT)
	# Execute MELCOR.
	print('ls is:')
	this_dir_list = sorted(os.listdir(this_dir), key=str.lower)
	print('started executing melcor at %s' % (time.asctime()))
	for listed_file in this_dir_list:
		(mode, ino, dev, nlink, uid, gid, size, atime, mtime, ctime) =
os.stat(str(listed_file))
		mod_date = datetime.datetime.fromtimestamp(float(mtime)).strftime("%B %d
%Y %X")
		print('Name: %s, Size: %s, Modified: %s' % (listed_file, str(size),
mod_date))
	sim1_exec_command = 'echo e | %s %s' % (os.path.join(MELCOR_ROOT, MELCOREXE),
MELCOR_TIME_INPUT)
	f = subprocess.run(sim1_exec_command, shell=True, stdout=subprocess.PIPE,
stderr=subprocess.STDOUT)
```

```
        print('stopped executing %s at %s' % (MELCOREXE, time.asctime()))
        print('ls is:')
        this_dir_list = sorted(os.listdir(this_dir), key=str.lower)
        for listed_file in this_dir_list:
                (mode, ino, dev, nlink, uid, gid, size, atime, mtime, ctime) =
os.stat(str(listed_file))
                mod_date = datetime.datetime.fromtimestamp(float(mtime)).strftime("%B %d
%Y %X")
                print('Name: %s, Size: %s, Modified: %s' % (listed_file, str(size),
mod_date))

        ###################################

        # Gather some attributes about the completed branch.
        melcor_message_file = 'tmi.msg'
        melcor_message_file_contents = open(melcor_message_file, 'r').readlines()
        for line in reversed(melcor_message_file_contents):
                if stop_word in line:
                        mystopping_code = line.split(stop_word)[1].split()[0]
                        break
        for line in reversed(melcor_message_file_contents):
                if line.startswith(' TIME='):
                        sim_elapsed = float(line.split(' TIME=')[1].split()[0])
                        break
        for line in reversed(melcor_message_file_contents):
                if line.startswith(' Normal termination  TIME='):
                        normal_term = float(line.split(' Normal termination
TIME=')[1].split()[0])
                        sim_elapsed = normal_term
                        break
                # Determine if the experiment end time has been reached
        if sim_elapsed > adaptvars.experiment_endtime:
                mystopping_code = "Experiment_Endpoint"

from_LSTS = open('LSTS.out', 'w')
from_LSTS.write('stopping_code= ' + mystopping_code + '\nsim time = ' + str(sim_elapsed))
from_LSTS.close()
        # Finding variables at objectives
```

## Editrules File:

```
// Name of the simulator template input files with variables to be replaced by ADAPT.
TemplateInputFile LSTS adaptvars.py.tpl

BranchInputFile LSTS adaptvars.py

// The files used to determine the branching code: Stoppingword <simulator> <filename>
<magic word> <word on line that contains magic word>
StoppingWord LSTS LSTS.out stopping_code= 2

// The characters used to designate ADAPT variables in the simulator template input
files.
VarSeparator LSTS "<" ">"

// The name of the simulators for the database.
// These should match the executable names and the file_name in the database.
SimulatorExecutable LSTS LSTS_LonePine.py

// The simulator to run for the root branch.
InitialSimulator LSTS

// Initial values not tied to a particular branching condition.
INIT STOPSIMULATOR FALSE // ADAPT stop CF
INIT SCRIBESTOPCONDITION Early_Detection_Point
```

```
// CST begins undamaged.
INIT HOLESIZE 0.0
INIT HOLETF FALSE

// The reactor starts at full power.
INIT SCRAM FALSE
INIT AFWTF FALSE

// ADV detected on entering PIDAS vs intake sabotage
INIT B_1_GEARTIME 10000
INIT B_2_GEARTIME 10000
INIT B_3_GEARTIME 10000
INIT B_4_GEARTIME 10000
INIT B_5_GEARTIME 10000
BranchingConditionName Early_Detection_Point Detection of Adversaries
BranchingSimulator Early_Detection_Point LSTS
BranchProbability  Early_Detection_Point Found_Early     0.5
BranchProbability  Early_Detection_Point Found_Late      0.5

// Found early.
Early_Detection_Point Found_Early SCRIBESTOPCONDITION Sabotage_CST
Early_Detection_Point Found_Early SCRAM   TRUE
Early_Detection_Point Found_Early AFWTF   TRUE
Early_Detection_Point Found_Early B_1_GEARTIME         Current
Early_Detection_Point Found_Early B_2_GEARTIME         Current
Early_Detection_Point Found_Early B_3_GEARTIME         Current
Early_Detection_Point Found_Early B_4_GEARTIME         Current
Early_Detection_Point Found_Early B_5_GEARTIME         Current

// Found late.
Early_Detection_Point Found_Late SCRIBESTOPCONDITION Destroy_Intake_Structure
// Add branching point at loss of intake structure
BranchingSimulator Destroy_Intake_Structure LSTS
BranchProbability Destroy_Intake_Structure Intake_Lost 1.0
Destroy_Intake_Structure Intake_Lost SCRIBESTOPCONDITION Sabotage_CST
Destroy_Intake_Structure Intake_Lost SCRAM   TRUE
Destroy_Intake_Structure Intake_Lost AFWTF   TRUE
Destroy_Intake_Structure Intake_Lost B_1_GEARTIME         Current
Destroy_Intake_Structure Intake_Lost B_2_GEARTIME         Current
Destroy_Intake_Structure Intake_Lost B_3_GEARTIME         Current
Destroy_Intake_Structure Intake_Lost B_4_GEARTIME         Current
Destroy_Intake_Structure Intake_Lost B_5_GEARTIME         Current

// CST Sabotage
BranchingConditionName Sabotage_CST Level of CST Damage
BranchingSimulator Sabotage_CST LSTS
BranchProbability Sabotage_CST Small_Hole 0.33
BranchProbability Sabotage_CST Medium_Hole 0.34
BranchProbability Sabotage_CST Large_Hole 0.33

Sabotage_CST Small_Hole HOLETF TRUE
Sabotage_CST Small_Hole HOLESIZE 0.33
Sabotage_CST Small_Hole SCRIBESTOPCONDITION Realign_AFW_Source

Sabotage_CST Medium_Hole HOLETF TRUE
Sabotage_CST Medium_Hole HOLESIZE 0.67
Sabotage_CST Medium_Hole SCRIBESTOPCONDITION Realign_AFW_Source

Sabotage_CST Large_Hole HOLETF TRUE
Sabotage_CST Large_Hole HOLESIZE 1.0
Sabotage_CST Large_Hole SCRIBESTOPCONDITION Realign_AFW_Source


INIT FLEXAVAIL TRUE
INIT FLEXATF TRUE
INIT FLEXBTF TRUE
```

```
// Only one branch to pass data from Scribe to MELCOR
BranchingSimulator A_1_Sabotage_FLEX LSTS
BranchProbability A_1_Sabotage_FLEX FLEX_Lost 1.0

A_1_Sabotage_FLEX FLEX_Lost FLEXAVAIL FALSE

// Combat occurs

INIT ENGAGEMENTS TRUE
INIT A_1_SKIPFLEX FALSE
INIT A_2_SKIPFLEX FALSE
INIT A_3_SKIPFLEX FALSE
INIT A_4_SKIPFLEX FALSE
INIT A_1_ALIVE TRUE
INIT A_2_ALIVE TRUE
INIT A_3_ALIVE TRUE
INIT A_4_ALIVE TRUE
INIT B_1_ALIVE TRUE
INIT B_2_ALIVE TRUE
INIT B_3_ALIVE TRUE
INIT B_4_ALIVE TRUE
INIT B_5_ALIVE TRUE

BranchingConditionName Engagement Outcome of Engagement
BranchingSimulator Engagement LSTS
BranchProbability Engagement ADV_SQUEAKER 0.5
BranchProbability Engagement ADV_ROUT 0.5

Engagement ADV_SQUEAKER ENGAGEMENTS FALSE // Only one modeled engagement
Engagement ADV_SQUEAKER B_1_ALIVE FALSE
Engagement ADV_SQUEAKER B_2_ALIVE FALSE
Engagement ADV_SQUEAKER B_3_ALIVE FALSE
Engagement ADV_SQUEAKER B_4_ALIVE FALSE
Engagement ADV_SQUEAKER B_5_ALIVE FALSE

Engagement ADV_SQUEAKER A_1_ALIVE TRUE
Engagement ADV_SQUEAKER A_2_ALIVE TRUE
Engagement ADV_SQUEAKER A_3_ALIVE FALSE
Engagement ADV_SQUEAKER A_4_ALIVE FALSE
Engagement ADV_SQUEAKER A_1_SKIPFLEX TRUE
Engagement ADV_SQUEAKER A_2_SKIPFLEX TRUE
Engagement ADV_SQUEAKER A_3_SKIPFLEX TRUE
Engagement ADV_SQUEAKER A_4_SKIPFLEX TRUE

Engagement ADV_ROUT ENGAGEMENTS FALSE // Only one modeled engagement
Engagement ADV_ROUT B_1_ALIVE FALSE
Engagement ADV_ROUT B_2_ALIVE FALSE
Engagement ADV_ROUT B_3_ALIVE FALSE
Engagement ADV_ROUT B_4_ALIVE FALSE
Engagement ADV_ROUT B_5_ALIVE FALSE

Engagement ADV_ROUT A_1_ALIVE TRUE
Engagement ADV_ROUT A_2_ALIVE TRUE
Engagement ADV_ROUT A_3_ALIVE TRUE
Engagement ADV_ROUT A_4_ALIVE FALSE

// BC for field action
INIT TEMPARMED TRUE
INIT ESCORT_ALIVE TRUE
INIT CR_OPERATOR_ALIVE TRUE
INIT ESCORT_DISPACHTIME 100000
INIT OPERATOR_FIELDTIME 100000

BranchingSimulator PRIMARY-TEMPERATURE LSTS
BranchProbability PRIMARY-TEMPERATURE Realign_Success 0.5
```

```
BranchProbability PRIMARY-TEMPERATURE Realign_Failure 0.5

PRIMARY-TEMPERATURE Realign_Success TEMPARMED FALSE
PRIMARY-TEMPERATURE Realign_Success STOPSIMULATOR FALSE
PRIMARY-TEMPERATURE Realign_Success SCRIBESTOPCONDITION Realign_AFW_Source
PRIMARY-TEMPERATURE Realign_Success A_1_ALIVE FALSE
PRIMARY-TEMPERATURE Realign_Success A_2_ALIVE FALSE
PRIMARY-TEMPERATURE Realign_Success A_3_ALIVE FALSE
PRIMARY-TEMPERATURE Realign_Success A_4_ALIVE FALSE
PRIMARY-TEMPERATURE Realign_Success ESCORT_DISPACHTIME Current
PRIMARY-TEMPERATURE Realign_Success OPERATOR_FIELDTIME Current

PRIMARY-TEMPERATURE Realign_Failure TEMPARMED FALSE
PRIMARY-TEMPERATURE Realign_Failure STOPSIMULATOR FALSE
PRIMARY-TEMPERATURE Realign_Failure SCRIBESTOPCONDITION Realign_AFW_Source
PRIMARY-TEMPERATURE Realign_Failure ESCORT_ALIVE FALSE
PRIMARY-TEMPERATURE Realign_Failure CR_OPERATOR_ALIVE FALSE

INIT REFILLTF FALSE
// New AFW source set
BranchingSimulator Realign_AFW_Source LSTS
BranchProbability Realign_AFW_Source New_Source 1.0

Realign_AFW_Source New_Source HOLETF FALSE
Realign_AFW_Source New_Source REFILLTF TRUE
```