SANDIA REPORT
SAND2017X-XXXX
Unlimited Release
Printed September 2017

System Theoretic Frameworks for Mitigating Risk Complexity in the Nuclear Fuel Cycle

Adam D. Williams, Doug M. Osborn, Katherine A. Jones, Elena A. Kalinina, Brian Cohn, Amir H. Mohagheghi, Mercy DeMenno, Maikael Thomas, M. Jordan Parks, Ethan Parks and Brian Jeantete

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology and Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: http://www.ntis.gov/search

SAND2017-10243
Printed September 2017
Unlimited Release

System Theoretic Frameworks for Mitigating Risk Complexity in the Nuclear Fuel Cycle

Adam D. Williams
Amir H. Mohagheghi
6833 Global Security Research & Analysis
Brian Cohn and Doug M. Osborn
8852 Severe Accident Analysis
Katherine A. Jones and Mercy DeMenno
8831 Operations Research & Computational Analysis
Elena A. Kalinina
8845 Storage and Transportation Technologies
Maikael Thomas
6832 International Safeguards and Engagements
Ethan Parks and M. Jordan Parks
6835 International Nuclear Security Engineering
Brian Jeantete
6522 Interactive Systems Simulation & Analysis

Sandia National Laboratories
P. O. Box 5800
Albuquerque, New Mexico 87185-MS1371

ABSTRACT

In response to the expansion of nuclear fuel cycle (NFC) activities—and the associated suite of risks—around the world, this project evaluated systems-based solutions for managing such risk complexity in multimodal and multi-jurisdictional international spent nuclear fuel (SNF) transportation. By better understanding systemic risks in SNF transportation, developing SNF transportation risk assessment frameworks, and evaluating these systems-based risk assessment frameworks, this research illustrated interdependency between safety, security, and safeguards risks is inherent in NFC activities and can go unidentified when each "S" is independently evaluated. Two novel system-theoretic analysis techniques—dynamic probabilistic risk assessment (DPRA) and system-theoretic process analysis (STPA)—provide integrated "3S" analysis to address these interdependencies and the research results suggest a need—and provide a way—to reprioritize United States engagement efforts to reduce global nuclear risks. Lastly, this research identifies areas where Sandia

National Laboratories can spearhead technical advances to reduce global nuclear dangers.

ACKNOWLEDGMENTS

The authors would like to thank the LDRD committee for the opportunity to conduct such challenging, but very rewarding, research. We also thank the Global Nuclear Assurance and Security (GNAS) leadership for their support through this project. We also are indebted to a group of hardworking student interns who assisted in various aspects of this project: Emma Johnson, Catherine Wright, and Anand Macherla. (Note: The project lead, Adam Williams, would like two personal acknowledgments. The first is to Dr. Amir Mohagheghi, whose vision, mentorship, and support were instrumental in completing this research. The second is to the members of my research team whose professionalism, intellectual curiosity, and hard work made this project a success.)

TABLE OF CONTENTS

FIGURES

TABLES

NOMENCLATURE

Abbreviation	Definition
3S	Safety, security, and safeguards
ADAPT	Analysis of Dynamic Accident Progression Trees
BNL	Brookhaven National Laboratory
BWR	boiling water reactor
COTS	commercial-off-the-shelf
DET	dynamic event trees
DOE	U.S. Department of Energy
DPRA	Dynamic probabilistic risk assessment
HCS	hierarchical control structure
HEU	highly enriched uranium
IAEA	International Atomic Energy Agency
MEI	maximum exposed individual
MIT	Massachusetts Institute of Technology
MUF	material unaccounted for
NFC	nuclear fuel cycle
NNSA	U.S. National Nuclear Security Administration
NPT	Non-Proliferation of Nuclear Weapons
OSU	Ohio State University
PIV	physical inventory verification
PRA	Probabilistic risk assessment
PWR	pressurized water reactor
SIR	state of increased risk
SME	subject matter expert
SNF	spent nuclear fuel
SQ	significant quantity
STAGE	Scenario Toolkit and Generation Environment
STAMP	System Theoretic Accident Model and Process
STPA	System theoretic process analysis
VESPA	Vulnerability evaluation simulating plausible attacks

(THIS PAGE IS INTENTIONALLY BLANK)

1. INTRODUCTION

Given how the increasing global demand for electricity and climate change concerns have expanded the use of nuclear fuel cycle (NFC) infrastructure around the world—and the associated suite of risks—this project evaluated a systems-based solution for managing the complex risks of the NFC. Combined with a multifaceted threat environment, this expanding NFC infrastructure results in increasingly complex security risks, as described by Olli Heinonen (former Deputy Director-General for Safeguards at the International Atomic Energy Agency and current Senior Advisor on Science and Nonproliferation at the Foundation for Defense of Democracies):

> *Safeguards, security, and safety* are commonly seen as *separate areas* in nuclear governance. While there are technical and legal reasons to justify this, they also *co-exist and are mutually reinforcing*. Each has a *synergetic effect on the other*, and authorities should carve out avenues for collaboration to contribute to the effectiveness of the nuclear order. For instance, *near real-time nuclear material accountancy and monitoring systems* provide valuable information about the location and status of nuclear material. This in turn is useful for *nuclear security* measures. Similarly, such information enhances *nuclear safety* by contributing as input to critical controls and locations of nuclear materials [1]. (Emphasis added)

For this research, this risk space was impeccably captured in the safety, security, and safeguards (3S) challenges of transporting spent nuclear fuel (SNF). In line with Dr. Heinonen's statement, developing a 3S system framework identified gaps, interactions, and conflicts that would be missed by the traditional approach of analyzing each 3S subsystem in isolation. To do so, this research adapted novel applications of two analytical approaches—dynamic probabilistic risk analysis (DPRA) and system-theoretic process analysis (STPA)—into an implementable framework, pushing the cutting edge of 3S research beyond conceptual efforts. Traditional SNF transportation evaluation methods for 3S are challenged by ignoring interdependencies and assuming time independence. In contrast, this research utilized system-theoretic approaches and dynamic risk assessment frameworks to assess, manage, mitigate, and reduce complex risks of SNF transportation with a time-dependent, dynamic control theoretic complex system model.

1.1. Motivation

The recent creation and development of new nuclear programs (e.g., United Arab Emirates and Vietnam) and increasingly popular "fuel take back" agreements as incentives for new nuclear energy programs suggests a significant increase in the amount of SNF to be transported, including transfers of SNF casks between transportation modes (e.g., road to rail to water) and across geopolitical or maritime borders. Further, this increases the likelihood that safety, security, and safeguards mitigation resources and regulations along approved international SNF transportation routes will be inconsistent.

Though limited in number, real cases suggest an increase in complexity for future international SNF transportation and motivate this research. For example, consider the spring 1996 shipment of spent highly enriched uranium (HEU) fuel from a research facility in Bogota to the Colombian coast for shipment back to the U.S. as part of a global program to swap HEU for low enriched uranium in research reactors. Decisions regarding this SNF shipment had to include mitigations

for complexities, such as strained governmental relationships between Colombia and the U.S., high guerilla activity during a period of severe civil unrest and navigating road, rail, or air travel infrastructure in various states of disrepair [2]. In addition, consider how the 2005 agreement between Moscow and Tehran for SNF from Iran's Bushehr nuclear power plant to be transported back to Russia also may involve diverse risks [3]. Simply looking at a world map suggests that these cases introduce a new, more complex set of risks, including overlaps in risk mitigation responsibilities (e.g., at ports or harbors) and conflicting objectives (e.g., national regulations for labeling hazardous materials on transportation routes), for international shipment of SNF [4].

Because current SNF transportation analyses heavily emphasize safety, lightly touch security, and typically ignore safeguards, this research created an analytical framework to perform a systems-based analysis for understanding risk complexity in SNF transportation with 3S analysis techniques.

1.1.1. Background

Despite the number of conceptual efforts on integrated 3S approaches, there has not been any serious research regarding systems analysis or modeling of the 3S system. Traditional SNF evaluation methods for safety, security, and safeguards are challenged by ignored interdependencies, stochastic assumptions, and time-independent analysis. Recent interest in how to integrate 3S prompted multiple studies from both international and domestic organizations, including Sandia National Laboratories, to include:

- Characterizing the current state of 3S integration at U.S. nuclear power plants [5];
- Integrating 3S into international nuclear infrastructure improvement programs [6];
- Proposing a conceptual systems approach to integrating 3S within the broader context of a civilian nuclear energy program [7]; and,
- Describing 3S as a preliminary framework for coordinating the safety, security, and safeguards regulatory requirements and combining the results of individual analyses. [8]

These recent efforts to characterize integrated 3S approaches have extended preliminary studies, but still remain in the conceptual space. One recent example leverages overlaps in regulations, procedures, and instrumentation between safety, security, and safeguards to offer "3SBD" as a potential resource savings for nuclear utilities. This study offers using data gathered on a shared video surveillance platform for perimeter monitoring (security), providing continuity of knowledge (safeguards), and detecting hazardous scenarios (safety), as an example [9]. A second recent example, vulnerability evaluation simulating plausible attacks (VESPA), uses traditional risk management approaches to integrate the 3S by effectively pairing sabotage with safety and theft with safeguards [10]. Both of these recent approaches mention—but offer no mitigations for—the increase in complexity from 3S analysis.

Considering SNF transportation as a complex socio-technical system offers a new paradigm by which to characterize and mitigate increasing risk complexity. Because risk stems from interactions between technical, human, and organizational influences within a complex system, reducing risk for specific scenarios or components may prove insufficient. Therefore, there is a need to evaluate the system as a whole to adequately characterize, evaluate, and manage

increasing risk complexity [11]. Two particular system-theoretic approaches have shown promise in mitigating risk complexity: DPRA and STPA.

1.2. Research Goals

This project aimed to research system-theoretic approaches and develop dynamic risk assessment frameworks for the NFC. Specifically, the project established complex system models and 3S risk mitigation strategies for international SNF transportation and demonstrated how to assess, manage, mitigate, and eliminate complex risks of SNF transportation. The following were the three research goals:

Research Goal #1: Understand systemic threats and risks related to SNF transportation:

- Identify gaps, interdependencies, conflicts, and leverage points of 3S.
- Develop relationships between 3S system properties and risk.

Research Goal #2: Develop SNF transportation risk assessment frameworks:

- Demonstrate simple DPRA- and STPA-based models for SNF transportation.
- Feasibility study on hypothetical, international SNF case.

Research Goal #3: Evaluate effectiveness of SNF system model and risk assessment framework:

- Compare the complex, socio-technical system model and risk assessment frameworks.
- Generate risk-mitigation strategies from case study.

1.3. Research Method

1.3.1. Case study

Because the goal of a case study is to "understand complex social phenomena…to focus on a 'case' and retain a holistic and real-world perspective" [12, p. 4], this research method seems to align with the goals described previously. A case study research method is useful and appropriate for answering "how" or "why" research questions—especially for real-world events within complex, dynamic environments. Per [12], collecting multiple sources of evidence, organizing analysis of the evidence, and building logical explanations within a single case can enhance research reliability and generalizability.

Yin characterizes three beneficial features of a case study [12]. First, a case study is useful to analyze situations in which there are many more variables than data points. Second, case study analysis builds from prior theoretical propositions to guide data collection and analysis. Third, a case study relies on multiple sources of evidence and analysis that illustrate how the data converges in a triangulating fashion toward useful conclusions.

Further, the case study method is useful for building theory and providing insight into specific causal mechanisms [13]. Rather than distilling or reducing complex cases down to a set of isolated variables for experimental hypothesis testing, case study research rests on the "central idea…that researchers constantly compare theory and data—iterating toward a theory which closely fits the data" [13, p. 541]. The better the data fits the theoretically developed causal

mechanisms, the more likely it can be expected for the same causal mechanisms in similar conditions or circumstances to have the same results. Case study generated theory is "particularly well-suited to new research areas…highly complementary to incremental theory building from normal science research" [13, p. 549]—and uniquely appropriate for exploring system-theoretic approaches to risk complexity in SNF transportation.

1.3.2. Hypothetical Case Description

This research required a hypothetical set of countries, material characteristics, and technologies to account for the range of classification sensitivities associated with exploring the risks of SNF transportation. Specifically, this example involves the physical transportation of SNF from an origin facility in Zamau, through the intermediary country of Famunda, to a destination facility in Kaznirra.

Figure 1 shows a regional map of our hypothetical SNF transport case study, which includes the following fictitious nations:

- **Zamau**, a non-weapons state signatory to the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) with a fairly robust nuclear enterprise that provides 12 percent of national electrical power (SNF origin);
- **Famunda**, a non-weapons state signatory to the NPT with rampant governmental corruption (SNF transit country); and,
- **Kaznirra**, a non-weapons state signatory to the NPT & Additional Protocol with a well-developed nuclear enterprise interested in making Site B a regional SNF repository (SNF destination).

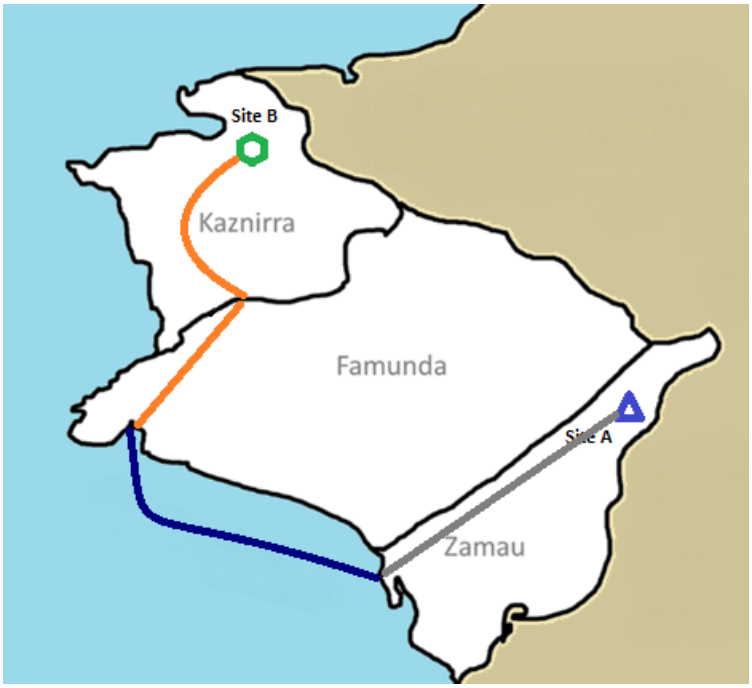

Figure 1. Regional Map (and Route) of Hypothetical SNF Transportation.

Similarly, this international SNF transportation route is multimodal and multi-jurisdictional, including:

- SNF cask is loaded at the origin facility (Site A) onto a rail car for transportation to the Port of Zamau (straight grey line);
- 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);
- 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); and
- SNF continues travelling by truck to the destination facility (Site B) in Kaznirra (curved orange line).

For additional details regarding the hypothetical countries; technical characteristics of the SNF, cask, or transportation vehicles; scenarios; or assumptions regarding the hypothetical case study, see "Hypothetical Case and Scenario Description of International Transportation of Spent Nuclear Fuel (SAND2017-TBD)" [14].

The details within this case description and scenarios of concern were briefed before a panel of subject matter experts from a range of disciplines (including spent fuel transportation, spent fuel management, nuclear safety, nuclear security, and nuclear safeguards). This audience indicated no glaring mistakes, omissions, or flawed logic within either the case description or scenarios.

1.3.3. Scenario 1

During transit through Zamau, the train is derailed due to a 40-foot section of missing track. The derailed train[1] is then opportunistically attacked by a state actor posing as a terrorist organization, who engages with the train's security force in a short firefight. In this scenario, if the attack is thwarted, the SNF shipment continues to its destination. However, if the attackers are successful, they quickly divert as many assemblies as necessary to obtain one significant quantity (SQ) of Pu from the fuel assembly, replace any missing material with dummy fuel rods, re-apply the containment seal, and create a radiological release by detonating TNT attached to a fuel rod to make the diversion appear to be an act of terrorism. Lastly, the remains of the SNF assemblies in the cask will eventually be shipped back to Site A, and Zamau will send a special report to the IAEA, detailing the incident. An IAEA inspector subsequently will inspect and examine the SNF shipment cask at Site A.

1.4. Analytical Thrusts

At the highest level, this research is designed to explore the hypothesis that integrated 3S approaches are improvements for managing complex risks in the NFC over traditionally isolated "S" approaches. Consider a broad meaning of the term "improvements" that includes the ability

[1] Per the relatively low track class (standards dictating railroad track quality) of Zamau's expansive railway network (i.e., gray portion of the SNF transportation route), and because train derailments are the most common type of rail incident [51], the first scenario for analysis included such an event.

to identify operational risks missed (gaps), illustrate interactions between risks and mitigations (interdependencies), characterize oppositional forces in operational risks (conflicts), and capture natural redundancies or compensatory effects to mitigate risks (leverage points). This research consisted of three broad thrusts. The first thrust was the development of a DPRA-based approach for 3S risk analysis (Section 2). The second (parallel) thrust was the development of a STPA-based approach comparing 3S versus individual "S" analyses (Section 3). Lastly, the third thrust was creating a new concept, coined "complex risk," to capture the interdependence of safety, security, and safeguards risks within an operational context (Section 4).

2. DYNAMIC PROBABILISTIC RISK ASSESSMENT (DPRA)

Probabilistic risk assessment (PRA) methods are traditionally used to inform decisions about nuclear risk. Such methodologies use fault trees and event trees to determine the probabilities, and possible evolutions of system behavior, from initiating from a basic event. Event trees are tools to model the possible ways failures (or other undesired actions) propagate through the system model and into various end states. These tools function by having a single branch representing a system's original state and moving forward through time to evaluate the system's response to periodic events, which may or may not occur. At these events, the event tree branches into multiple paths, each representing different potential outcomes of the given event, which usually consists of success or failure of a subsystem. The probabilities for these different outcomes are determined using fault trees, which are a way of calculating the necessary conditions for subsystems to fail.

Standard fault tree and event tree methods, which by nature are static, have limited applicability for some scenarios. Generally, these concerns are focused on the rigid nature of the event logic being followed and how this analysis assumes a single order of events for a given scenario, one that is typically based on expert elicitation. However, there are scenarios in which the order of events is uncertain and the specific order of sub-events can have substantial effects on the evolution of the scenario. For example, the time necessary for offsite local law enforcement officers to arrive at a site in an event requiring a response can play a substantial role in the progression of ensuring steps in the event. If local law enforcement arrives quickly (e.g., before any transport security escorts are killed), then the combined security response forces are much more likely to deter or neutralize adversaries.

In response, dynamic probabilistic risk assessment (DPRA) is a methodology that creates a framework to analyze the evolution of event trees that describe various paths between initiating events and possible end states. This framework uses system-level models to represent the status of the system in question and determines its possible evolutions during a scenario. This is a "bottom-up" technique that statistically evaluates simulation run-based data from deterministic approaches to generate insights about risk.

2.1. Explanation

DPRA can use several analytical methods, which have certain common characteristics:

- A deterministic system model or set of models with outputs that clearly distinguish successful and unsuccessful endpoints;
- A driver of system models that can run codes with different input files; and,
- A systematic algorithm to determine the probabilities of different system configurations, including success or failure of components or processes, and explore the resulting uncertainty space.

The most-common DPRA analysis techniques are dynamic event trees (DETs), which are similar to event trees that do not have their structure preset. Instead, the system model is tracked and the DET branches at pre-specified conditions or events. When this occurs, the logic for the branching condition in question determines the number of possible resulting branches and speaks to the associated probabilities that any one of these branches will be realized. The resulting DET

then is solved following well-established event tree analysis processes. This process is repeated until either the logical end conditions of the tree are achieved or pre-determined stopping conditions are reached.

2.1.1. DPRA Methodology

DPRA employs DETs for the systematic and automated assessment of possible scenarios arising from uncertainties within the complex system model. In this manner, DPRA can better account for both epistemic (e.g., arising from the model) and aleatory (e.g., arising stochasticity in the complex system) uncertainties to provide higher fidelity analytical conclusions for complex system analysis. More specifically, the DPRA research thrust used the Analysis of Dynamic Accident Progression Trees (ADAPT) software to generate DETs by acting as an overall scenario scheduler to coordinate the complex system model-related inputs and outputs between three different software codes (that support traditionally isolated "S" analysis):

- **RADTRAN**[2], an internationally accepted program and code for evaluating the safety risks of transporting radioactive materials;
- **STAGE**, a Sandia-specific application of a commercial modeling and simulation program for evaluating security risks in terms of physical protection system effectiveness; and,
- **PRCALC**, a Markov Chain-based code (developed by Brookhaven National Laboratory) for evaluating various risks associated with safeguarding nuclear materials.

2.1.2. ADAPT Simulation Software

ADAPT is a DET code that was developed jointly by Sandia National Laboratories and The Ohio State University to coordinate with a wide variety of codes. As such, ADAPT has a small number of assumptions regarding coordination with other software codes:

- They must be able to be run from the command line;
- They must stop when a branching condition is reached;
- They must record the branching condition that occurred; and,
- They must restart from the previous point with a changed set of parameters.

The ADAPT code consists of two processes. The first is the *adapt-server*, which controls the branches of the DET, runs the models, and collects the related output. The second is the *adapt-webmin*, which provides a browser interface for the user to launch experiments and collect results. Both of these processes are connected to a central database, which stores the results of the simulation runs.

To use the *adapt-server* and *adapt-webmin* functionality, ADAPT requires a number of additional files beyond the different simulator codes and their input files. ADAPT requires a template input file for each simulator, an *editrules* file, and a *wrapper* file designed for the specific combination of simulators used in a single simulation run. Additionally, if ADAPT is

[2] Copyright Sandia National Laboratories 2006. RADTRAN 6.10, from 2014, is the version used for this effort.

being controlled through the web interface, which is the suggested method, it requires a *webwrapper* file in addition to the other files to submit the correct options necessary for the analysis job.

The template files for different simulators are designed to provide location data to ADAPT for the modifiable variables within a simulation. Each ADAPT variable is distinguished from the input file through unique starting and ending characters. For example, brace characters ("{" and "}") are often used to offset ADAPT variables, as in Figure 3. By replacing the ADAPT variables with the appropriate range of values, the template file is executed in the simulation.

The *wrapper* file is a code at the heart of ADAPT analysis. Written using the Bash scripting language, this file describes the behavior of ADAPT at each branch of the DET and is executed every time ADAPT branches. The *wrapper* file determines how the edit rules apply to a specific branch and creates a related input file using the template file for that simulator. After creating the input file, the *wrapper* then executes the simulator. The output file of the simulator is read by the *wrapper* and a unique *stopping code* included in the output is then executed. This *stopping code* describes the stopping logic of the simulator and is interpreted by the *wrapper* file to determine if the branch is terminal or if it has additional branches that need to be generated to continue the analysis. In the event that there are such additional branches to be created, the wrapper applies the edit rules and executes the necessary files to generate further branches. Figure 2 illustrates this process.

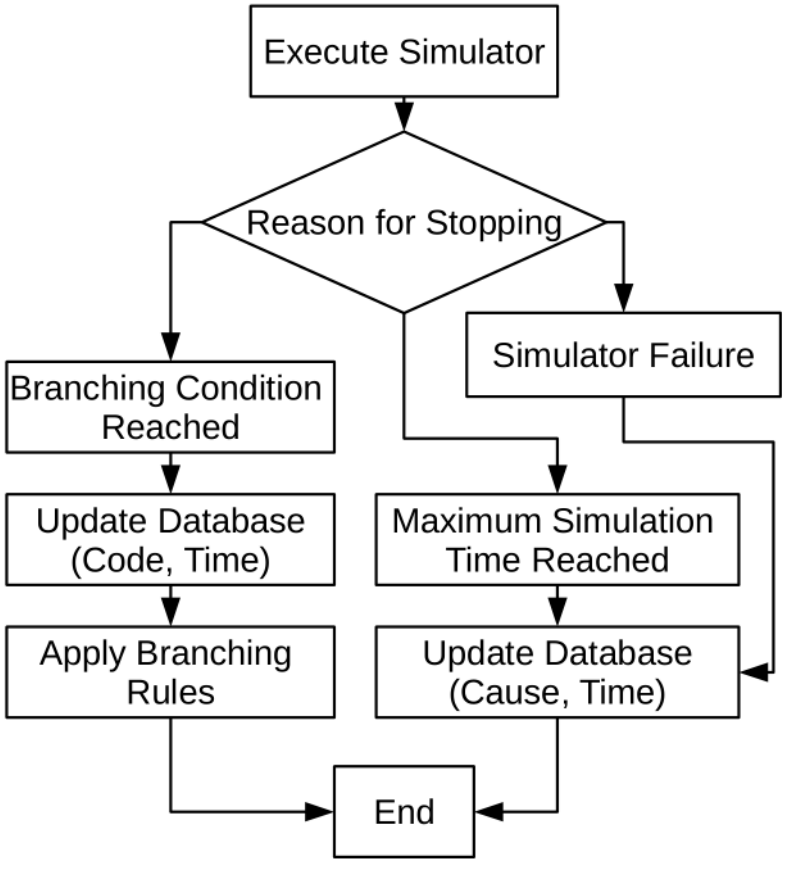

Figure 2. Representation of an ADAPT Branch from [15].

The *editrules* file provides ADAPT with the options for how ADAPT variables in template files should be replaced, based on the scenario under analysis. These are known as branching rules. Additionally, for analyses that use multiple simulators, the *editrules* describe which simulator is run for each branch for the DET. The *editrules* file consists of sets of changes to make to input files for a given *stopping code*, representing different events that can occur within a simulation. For example, Figure 3 shows the branching rules that describe the branching that occurs in the DET based on the size of the derailment accident for STAGE and RADTRAN jointly (Scenario 1 introduced previously). In the figure, black and orange text are the actual variables and values and the green text is the related physical descriptions.

```
// ================================ 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
```

Figure 3. Sample of the *editrules* File Describing Branching Based on Accident Severity.

Each column of the *editrules* has a different meaning. The first column lists the *stopping code*, passed to the *editrules* from the output of an earlier simulator through the *wrapper*, that corresponds to the event in question. The second describes the branch that is being changed in that line of the code. In Figure 3, there are three different branches of accident severity (as expressed in terms of release particulate, volatile and gaseous fractions), corresponding to the size of the accident caused by the derailment. The next column describes which ADAPT variable is being changed in that line. Notably, different branches have freedom to change completely different ADAPT variables and do not depend on which ADAPT variables are being changed by other branches. Notice, however, that the T3, T4, and T5 strings are not given to the input file as-is. Earlier in the *editrules,* file these were defined as tables with multiple values and probabilities. As such, ADAPT creates additional branches for each of these table entries. Text after "//" is an optional comment and not executed by ADAPT.

2.1.2.1. RADTRAN Methodology and Simulation Code

RADTRAN is the national standard for estimating transportation-related radiation doses and risks by combining user-determined meteorological, packaging, demographic, transportation, and material data with health physics data to calculate the expected radiological consequences and accident risk of transporting radioactive material. Further, RADTRAN has been used

extensively by U.S. federal, state, and local agencies and contractors, international government agencies and private contractors, universities, and individuals, including in [16] and [17].

2.1.2.2. STAGE Methodology and Simulation Code

Sandia has used the commercial-off-the-shelf (COTS) Presagis International computer combat model Scenario Toolkit and Generation Environment (STAGE) [18] to develop a novel vulnerability analysis tool to aid in the design and evaluation of nuclear security applications. STAGE enables users to focus more on the complex behaviors of the scenario and less on plotting the exact course of entities; allows entities within STAGE to dynamically plan paths, recognize and avoid obstacles or harsh terrain; and, stay on defined pathways, such as roads or sidewalks [18]. The ability to react with intelligent behaviors to dynamic simulation environment changes at the entity level exemplifies the overall flexibility that STAGE has in modeling higher-fidelity security analysis for nuclear applications [19].

2.1.2.3. PRCALC Methodology and Simulation Code

The DPRA thrust also evaluated software named PRCALC (created at Brookhaven National Laboratory [20]), which computes the probabilities of proliferation success, diversion detection, and diversion failure at a given stage, for safeguards in the ADAPT analysis. The complexity of addressing safeguards suggests the importance of maintaining continuity and the quality of knowledge (beyond current best practices) along international SNF transportation routes, and Mladineo, et. al., suggested Markov chain models as a method to do just that [21]. A Markov model breaks a time-variant scenario into discrete stages (or states) using a directed graph with transition parameters defining the probability of advancing to the next stage. Future and past states of the Markov process are considered independent of the present state. In addition, this method can compute probabilistic measures that account for a range of uncertainties in the complexity inherent in meeting safeguards obligations in the international SNF transportation.

2.1.3. ADAPT Edit and Branching Rules

As a DET code, ADAPT functions through a branching scheme. ADAPT launches the initial simulator as a single branch, detects when the simulator finished, and reads the output file to determine which branching condition occurred. These branching conditions can be based on a set of conditions within the system or at a scenario time. When a branching condition is found, the *editrules* file is consulted, as described in Section 2.1.2, to determine how the scenario develops and how many additional branches are created.

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. For Scenario 1, branching rules were created to modify different sets of codes. Some conditions purely modify an individual code, 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 directly, such as branching on the accident severity. This branching condition affects the radioactive release in RADTRAN, the number of available response forces, and the ability to access the cask in STAGE and the amount of time required in PRCALC to re-seal the cask for transport and return it to an inspection site for safeguards analysis. Table 1 summarizes the different branching conditions modeled and their effects.

Table 1. Representative Set of DPRA Branching Rules to Link RADTRAN, STAGE, and PRCALC in the ADAPT Software.

Branching Condition	RADTRAN Effects	STAGE Effects	PRCALC Effects
Cask Inventory: Burnup, Age	• Alters public consequences in the event of a release	—	• Changes attractiveness of material • Affects physical obstacles for diversion
Degree of Notice Given to Local Law Enforcement	• Reduces public evacuation time in the event of a release	• Shortens time for arrival of offsite reinforcements • Potentially increases ability of adversaries to gather and plan, due to leaks of route	—
Discovery of Damage to Track	• Allows for 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 • Increases the amount of time necessary for adversaries to arrive at the cask due to wreckage	• Increases the amount of time necessary to prepare cask for further transportation
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	• Sponsored attacks are a greater risk for diversion of the fuel as a goal
Time Necessary to Return Cask for Inspection	—	—	• Increased travel to an inspection site reduces the timeliness of safeguards reporting

2.2. Results from International SNF Transportation Analysis[3]

Each of these three phases of the scenario timeline have been analyzed with their respective software code. For Phase 1 using RADTRAN, the derailment accident was modeled for 12 different SNF configurations among burnups and fuel ages for both pressurized water reactor (PWR) and boiling water reactor (BWR) fuel types (see Appendix B for details). The resulting release fraction analysis, shown in Table 2, illustrates how such consequences could be amplified when accounting for Phase 2.

Table 2. RADTRAN Release Fractions[4] Related to Safety Risk for the Train Derailment Scenario.

Group	Release Fraction		Total Release Fraction	Aerosol Fraction	Respirable Fraction	Total Respirable
	From Rods	From Cask				
Gas	0.12	*M*x0.8	*M*x0.096	1	1	*M*x0.096
CRUD	1	0.001	0.001	1	0.05	$5*10^{-5}$
Particle	*N*x $4.8*10^{-6}$	*M*x0.7	*N*x*M*x $3.36*10^{-6}$	1	0.05	*N*x*M*x $1.68*10^{-7}$
Volatile	*N*x $3.0*10^{-5}$	*M*x0.5	*N*x*M*x $1.5*10^{-5}$	1	0.05	*N*x*M* $7.5*10^{-7}$

Similarly, STAGE evaluated Phase 2 as a characteristic attack on the SNF cask by a small, well-equipped adversary force. Here, the number of adversary attackers and response force members were varied; the first to indicate the uncertainty in actual attack details, and the latter to model the potential incapacitation of response force members from the derailment. Table 3 [A] and [B] illustrate how the probability of neutralization and average time on the task by an adversary changes across the difference configurations modeled, which provides insight into where ADAPT can insert RADTRAN outputs as inputs into the STAGE analysis.

Table 3. STAGE Generated Output Measures Related to Security Risk for the Train Derailment Scenario.

[A] Average P_N					[B] Average Time on Task (%)				
		Responders					Responders		
		2	4	8			2	4	8
Adversaries	3	43.4%	100.0%	100.0%	Adversaries	3	85.6%	56.4%	60.7%
	5	47.5%	96.0%	100.0%		5	82.7%	72.9%	68.5%
	7	19.2%	65.0%	93.0%		7	90.5%	87.1%	86.1%

[3] Many of these results derived from executing the individual software codes for safety, security, and safeguards were previously published (and explained in more detail) in the conference papers listed in Appendix A.

[4] More specifically, for particles and volatiles (from rods to cask): *N* times higher than in NUREG-2125 [16]; gases, particles, and volatiles (from cask to environment): *M* higher than in NUREG-2125 (M<N); *M* and *N* depend on the attack severity (i.e., evaluated by STAGE).

Lastly, PRCALC analyzed Phase 3 as an assumed successful elimination of the response forces by the adversaries, who then aim to divert a significant quantity of special nuclear material from the SNF cask and replace several fuel rods with dummy rods. The time varying probabilities of diversion failure and proliferation success probabilities (e.g., represented in the PWR configuration with 25-year aged with 60 GWD/MTU burnup in Figure 4) are attributable to the amount of Pu in the transport cask, and the model selection of a fixed intrinsic barrier that does not cause significant delay to proliferation [22]. Again, the selection of this particular intrinsic barrier indicates how ADAPT can insert STAGE outputs as inputs into the PRCALC analysis.

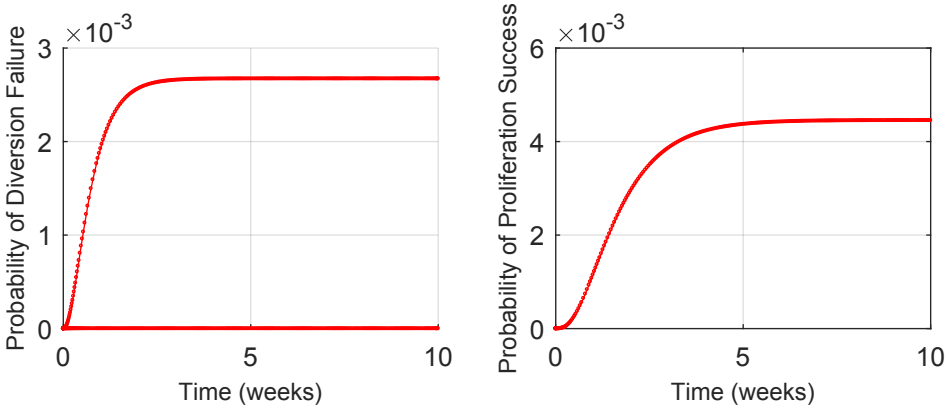

Figure 4. PRCALC Generated Output Measures Related to Safeguards Risk for the Train Derailment Scenario [22].

From here, the DPRA thrust focused on determining conditions in which the scenario might branch between different potential evolutions for the integrated 3S analysis. This analysis begins at the derailment (Phase 1) with RADTRAN, which does not have dynamic capabilities, and travels forward in (simulated) time. Branching in Phase 1 cannot be based on conditions that develop during the simulation, therefore ADAPT is used to perform branching similarly to a classical event tree, where the analysis is split along predefined junctions. These branches include:

- Different fuel characteristics (e.g., different fuel configurations affect the consequences in RADTRAN and STAGE differently, and also contain different quantities of fissionable material, which influences PRCALC); and,
- Multiple sizes of the accident (e.g., the more severe the accident, the greater potential for radioactive release and the more difficult for the response forces to perform in STAGE).

Because Phase 2 used the dynamic software code STAGE, branching could occur at specific instances in time, and result in multiple possible paths. Here, such conditions that defined this branching include:

- Between adversaries being state-sponsored or non-state actors (e.g., assumptions of greater financial and technical capabilities for the former influence both STAGE and PRCALC analysis); and,
- The degree of wreckage and habitability of the area around the cask (e.g., the terrain immediately around the canister may include different levels of hazards blocking access to the cask or to engaging the adversaries).

Lastly, Phase 3 used the results from the STAGE analysis (itself informed by the RADTRAN analysis) to evaluate state-sponsored adversaries with the goal of diverting spent fuel and detection efforts by IAEA inspectors—and the associated branching occurred in relation to the different states in the PRCALC Markov model.

2.3. 3S Meta-Analysis

For this research thrust, the research evaluated the differences (in terms of gaps, interdependencies, conflicts and leverage points) that emerged when evaluating "risk" in the international transportation of SNF with DPRA using an integrated 3S approach (Figure 5). The first ADAPT-based integrated analysis 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 this dynamic analysis, with more than 20,000 terminal states. This analysis calculated the radioactive release 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.

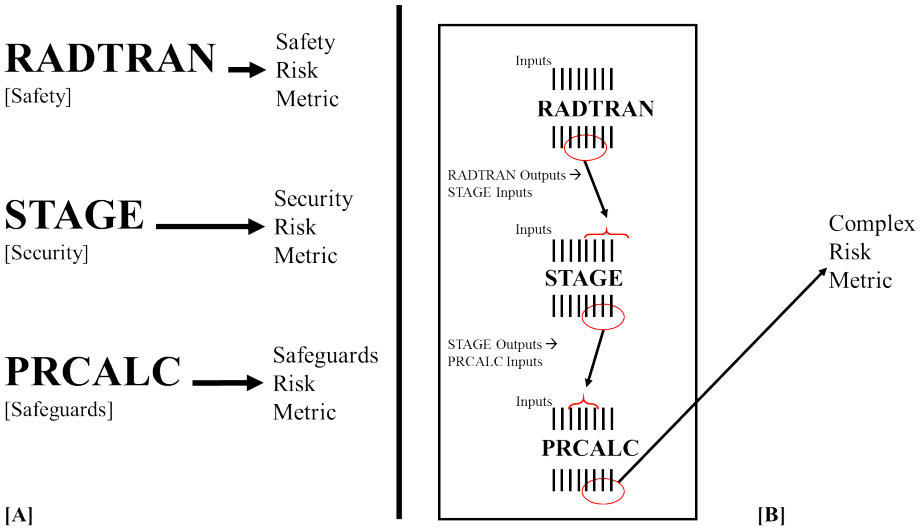

Figure 5. The DPRA Research Framework, via Representative Individual Characteristic-Specific Risk Analyses (A) and 3S Complex Risk (B) ADAPT Analysis.

For Scenario 1, the branching occurred in chronological order for ease of understanding. This is a construct of this scenario, though dynamic codes can have their branching occur in chronological order for each given instance without this order being known *a priori.* As each branch carried its attendant conditional probability, the overall probability of a branch is calculated based on the probabilities of all preceding branches.

The dose released in Phase 1, as the maximum exposed individual, is given in Table 4[A]. Dose calculations depended on the size of the accident, which affected the release fractions (as described in Table 2), and the advanced notice given to local law enforcement, which affects the evacuation time for nearby members of the public. In Phase 2, the probability of neutralization 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 4[B] illustrates P_N for the overall scenario.

Table 4. Combined RADTRAN-STAGE Scenario Output Measures.

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

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 branching condition is on the degree of advanced notice given to local law enforcement. To determine the effects of giving more information to local law enforcement, 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. Table 4 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 local law enforcement.

A manual investigation of a subsection of the results highlighted one interesting interaction between the safety and security analysis: that of hazards around the cask making it more difficult to access. A time penalty applied to the adversaries breaching the cask represented this additional difficulty. 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.

A subset of 96 simulation runs were considered in this analysis; 72 with no time penalty 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. This scenario used the same victory conditions for each side of the engagement as the individual STAGE analysis section. 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 5 shows P_N for no time penalty and a time penalty of 40 seconds.

Table 5. Average Probability of Neutralization (P_N) for the Subset of Simulation Runs for Scenario 1 that Considered How the Additional Wreckage and Fires Resulting from the Train Derailment Made Accessing the SNF Cask More Difficult for the Adversary and Provided Offsite Responders Additional Time to Arrive for Interruption and Neutralization.

Time Penalty	
0s	**40s**
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 were late to arrive on scene 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 this simulation 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, which reduced their 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, PRCALC 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 Phase 3, 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, security, and safeguards 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 3S meta-analysis argues that DPRA can be extended to better address the growing risk complexity dynamic that 21st century environments pose to international SNF transportation (and likely other NFC activities).

(THIS PAGE IS INTENTIONALLY BLANK)

3. SYSTEM THEORETIC PROCESS ANALYSIS (STPA)

STPA combines the engineered safety ideas of hierarchy, emergence, control, and communication into a new paradigm for understanding safety (and other emergent system properties) in large, complex systems. The System Theoretic Accident Model and Process (STAMP) is a model of causation for complex, socio-technical systems. In STAMP, a system is considered to be composed of interrelated components that maintain dynamic equilibrium through information and control feedback loops that enable it to adapt to changes in itself (or its environment) to achieve its objective. In this causality model, system losses result from flawed interactions between physical components, engineering activities, operational mission, organizational structures and social factors [23] [24].

STAMP further argues that desired behaviors of complex systems can be redefined as the ability of a system to maintain a state that eliminates losses resulting from migrating into states of increased risk and experiencing external events (e.g., the backup generators being located at sea-level and the tsunami at Fukushima). This shifts the analytical paradigm from preventing failures to enforcing constraints and emphasizes three fundamental concepts to eliminate, minimize, or mitigate states of increased risk:

- **Constraints**: Constraints are goals or set points by which higher levels within a hierarchy exhibit control of activities at lower levels based on the current understanding of the system being controlled [24].

- **Control structures**: Hierarchical organizational structure whereby the entire socio-technical system enforces constraints to avoid undesired states through accurate and timely communication [23].

- **Process models**: Current understanding of the variables, relationships between them, the current system state, and the processes that can change the state of the system (e.g., "mental map" or digital abstraction) [23].

Further, STPA is an analysis technique built on STAMP that identifies undesired system states across technical (physical and cyber) system elements; component interactions; cognitively complex human decision-making errors; and social, organizational, and management factors related to the system. In this regard, STPA does not seek to rank or prioritize the hazards that are identified; rather, it provides decision-makers and designers with additional information on which to implement technologies and create protocols to allow complex systems to operate free from unacceptable losses [23].

In general, STPA can be broken into two broad steps [23]. The first identifies potential inadequate control actions that could lead to a hazardous state, which can result when:

- Unsafe control commands are issued;

- Required safety control actions are not issued;

- Correct safety control actions are provided too early, too late, or in the wrong order; or,

- Control actions are stopped too soon (or too late), causing inadequate enforcement of safety constraints.

The second step to STPA is to determine, specifically, how each potentially unsafe control action identified in the previous step could occur. Related inadequate safety actions could include, but not be limited to, an incorrect operational state command issued; delay in safety system component confirming desired operational state; incorrect system state not detected; or, inaccurate feedback on the operational state of the system. Here, the STAMP-derived hierarchical control structure, standard operating procedures, and observations are combined to identify realistic causal scenarios for possible logical violations of control actions. STPA might identify several different causal scenarios for each logical category of control action violation (e.g., STPA Step 1). This suggests that mitigating potential control action violations can eliminate multiple causal scenarios for a hazard, including those often missed by traditional safety and hazard analysis techniques.

Williams argued that STPA could be applied to nuclear fuel cycle activities, where negative events result from interactions between system components that violate design constraints [25]. Similar to the ongoing evolution in engineered safety, "the fast pace of technological change," "reduced ability to learn from experience," "changing nature of [*security or safeguards*] incidents and [*adversaries or malicious actors*]," "new types of [*vulnerabilities or diversion opportunities*]," and "increasing complexity and coupling" [23, pp. 3-4] support system-theoretic approaches for the design, analysis, and implementation of nuclear facilities in today's environment. Safety, security, and safeguards are recast as both emergent systems properties and control problems regarding appropriate responses of NFC activities to "component failures, external disturbances, or dysfunctional interactions among system components" [24, p. 2].

3.1. Explanation

Figure 6 summarizes the STAMP/STPA process used in this research. Each step will be further explained in Section 3.2 using Scenario 1 data.

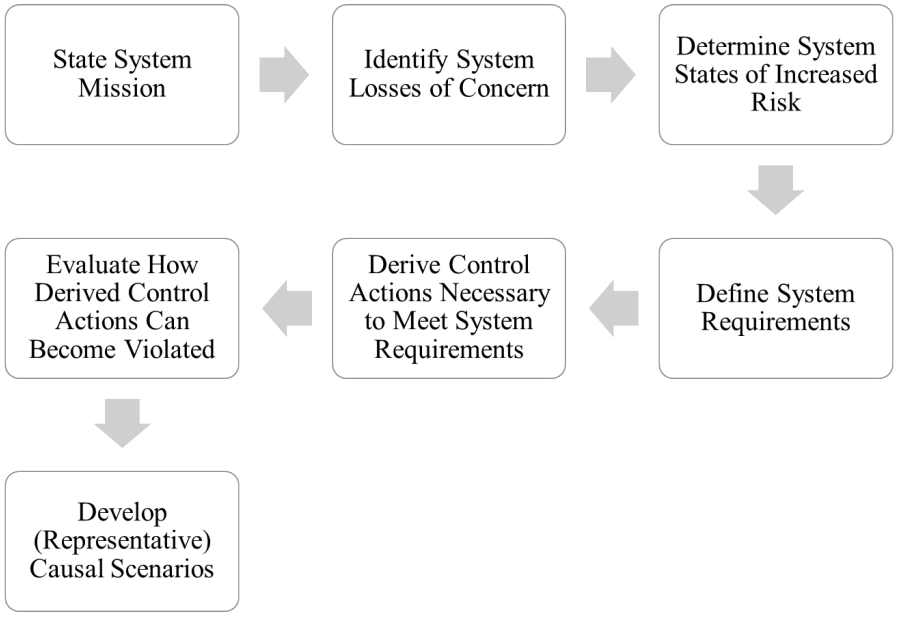

Figure 6. Summary of the Logic Supporting STAMP-Based Analysis Techniques for Evaluating Emergent, System-Level Properties.

3.1.1. STPA Applied to Safety

Over the last five years, STPA has been successfully applied to hazard analysis and system safety across a broad range of socio-technical systems, including in the aviation [26] [23], space [27] [24], automotive [28] [29], medical [30] [31], and nuclear power [32] [33] domains.

3.1.2. STPA Applied to Security

Similarly, recent work in critical infrastructure [34], cyber [35] [36], port security [37], and nuclear security [25] has argued that the theoretical foundation of STAMP and STPA is highly suitable for security applications. Further, Young [36] provided the first rigorous application of STPA to security as an emergent property and concluded that this approach provides a rigorous, structured problem-framing process, is able to include a wider range of underlying technical and operational influences, and is effective on real systems. In another study, Williams [37] demonstrated the ability of STPA to refocus improvement efforts away from concentric layers of security and toward controllable security control actions that allow security to be "embedded" in everyday work practices.

3.1.3. STPA Applied to Safeguards

Prior to this study, there were no identified applications of STPA to nuclear safeguards in the open literature.

3.2. Results from International SNF Transportation Analysis

State System Mission (describe the desired set of outcomes for the system to achieve)**:**

For the international transportation of SNF, the mission is to physically move SNF from an origin facility to a destination facility without disruption to selected and approved routes, timelines, and operations.

State System Losses of Concern (describe broad categories of undesired outcomes related to the system attempting to achieve its mission)**:**

STAMP defines unacceptable losses as the results of a system entering a state of increased risk and experiencing an external event, and treats them as the benchmarks for describing undesired behavior. Additionally, in STAMP, traditional losses identified in other analysis techniques are captured in higher-level, broader categories of unacceptable losses, which also provides an opportunity to include real-life concerns outside the scope of traditional approaches. As such, there may be varying timescale differences between what is "normally" considered a loss and what STAMP describes as a loss. For example, in safety analysis, loss of human life results from acute radiation dose in the timescale of weeks or months, whereas in safeguards, loss of human life results from the detonation of a nuclear material-related weapon, which take an order of years to manufacture. For example, consider Table 6, which summarizes losses for the hypothetical international SNF transportation case described in this research.

Table 6. STAMP-Based Descriptions of High-Level Losses for International SNF Transportation.

Losses	Representative Examples of Typical Metrics Captured in Traditional Safety, Security[5] and/or Safeguards Analysis

Human serious injury or loss of life (L1)	• Individual inhalation dose limits • Individual digestion dose limits • Individual skin absorption dose limits • Public radiation dose at regulated boundary around SNF
Environmental contamination[6] (L2)	• Land contamination (e.g., loss of use of farmland) • Dose of animals (e.g., endangered wildlife or livestock) • Inhabitability of structures[7] (e.g., irradiated buildings rendered usable)
Significant damage to infrastructure (L3)	• Kinetic damage • Fire damage • Hydrostatic damage
Significant loss of revenue (L4)	• Loss of SNF in entirety • Cost to repair access to SNF (e.g., within the cask) • Cost of an incomplete transportation route (e.g., returning to origin facility) • Cost for environmental cleanup, political reparations, and/or individual legal cases
Reputational/ professional confidence (L5)	• Reduced follow-on/additional SNF transportation work (e.g., loss of reputation) • Reduced usage of nuclear materials for civilian purposes (e.g., loss of professional reputation of the civilian NFC facilities)[8]
Non-adherence to IAEA obligations (L6)	• Untimely nuclear material reporting • Inaccurate nuclear material reporting • Unacceptable variance in nuclear material declarations

Determine System States of Increased Risk (use state-space characteristics to describe how system can exhibit increasingly risky behavior, moving it closer to experiencing an unacceptable loss):

Here, the STAMP causality model translates these high-level losses into related system states of increased risk (Table 8). Table 7 lists states of increased risk considered for this scenario.

Table 7. States of Increased Risk Derived from Losses Associated with International SNF Transportation.

State of Increased Risk	SIR Description	Associated Losses
SIR1	Unplanned radiological release from the cask	L1, L2, L3, L4, L5, L6
SIR2	Population/individual normal operations exposure limits exceeded	L1, L2, L3, L4
SIR3	Unconstrained movement of the cask (runaway cask)	L1, L2, L3, L4, L5

[5] We purposefully do not include "loss of material" as a high-level loss, as (1) the loss of SNF itself is a precursor to actual losses (e.g., loss of revenue) and (2) because the assumed nefarious end goal of an adversary is related to detonation (e.g., RED, RDD, IND, or NW), which results in other losses listed above (e.g., loss of human life, environmental contamination, or damage to infrastructure).

[6] An additional increased "risk state" results from potential overexposure to radiation during normal operations of non-dedicated transportation vehicles was not considered in our scenario/analysis because all transportation vehicles were assumed to be dedicated.

[7] Per standard assumptions in RADTRAN analysis, the limit for acceptable contamination levels is the population can return after 50 years.

[8] Similar in kind to the adage, adopted as a sort of unofficial motto for the past few IAEA Director Generals, "a nuclear accident anywhere is an accident everywhere."

SIR4	Transportation vehicle exceeds regulated speed limits	L1, L2, L4
SIR5	Unauthorized access of cask	L1, L2, L3, L4, L5, L6
SIR6	Unauthorized access of transportation vehicle	L1, L4, L5, L6
SIR7	Transportation vehicle stopped longer than expected	L1, L2, L3, L4
SIR8	Transportation vehicle traveling slower than scheduled	L2, L3, L5
SIR9	Unverified transfer of armed security responsibility	L1, L2, L3, L6
SIR10	Loss of "continuity of knowledge" of SNF material status	L1, L2, L3, L4, L5, L6
SIR11	Untimely reporting of SNF arrival	L5, L6
SIR12	Unknown state of rods inside cask	L1, L2, L3, L4, L5, L6

These states of increased risk are known as hazards in safety terms [23], vulnerabilities in security terms [37], and proliferation states in safeguards [22] (Table 8). For example, if there is unauthorized access to the SNF during the transport, the shipment could experience a loss—whether from the intentional use of explosives or unintentional closing of a pressure release valve. For both of these instances, if the unauthorized access had been prevented (through technical, administrative and/or systemic controls), then the shipment is less likely to experience a loss—even when responding to an external event.

Table 8. Representative Set of STAMP-Derived States of Increased Risk (and their Related Losses) for Safety, Security, and Safeguards of International SNF Transportation.

System States of Increased Risk		
Increased *hazardous* state	**Increased *vulnerable* state**	**Increased *proliferation* state**
Unplanned radiological release from the cask[9]	Unauthorized access of cask[5]	Loss of "continuity of knowledge" of SNF material status[5,10]
N/A	Unauthorized access of transportation vehicle	Loss of "continuity of knowledge" of SNF location[11]
Population/individual normal operations exposure limits exceeded[12]	Transportation vehicle stopped longer than expected	N/A
N/A	Transportation vehicle traveling slower than scheduled	Untimely reporting of SNF arrival
Unconstrained movement of the cask (runaway cask)	N/A	N/A
N/A	Unverified transfer of armed security responsibility	N/A
Transportation vehicle exceeds regulated speed limits	N/A	N/A
N/A	N/A	Untimely reporting of SNF removal

Define System Requirements (describe the necessary conditions for the system to avoid states of increased risk):

These states of increased risk help identify requirements for system behavior to avoid these states and achieve its overall mission. These requirements then act as both physical and procedural constraints on system design and operations to guide systemic behavior toward achieving the mission, while avoiding states of increased risk. These high-level requirements then serve as the rubric for evaluating the benefits of additional, removed, or modified requirements or actions. A representative set of high-level system requirements for the hypothetical international transportation of SNF case are described in the third column of Table 9.

Derive Control Actions Necessary to Meet System Requirements (identify control actions for each controller within the sociotechnical system model necessary related to meeting the higher-level system requirements)**:**

Illustrated in the hierarchical control structure (HCS) shown in Figure 7 (and in more detail in Appendix C; note that the inbound arrows represent controls or commands and outbound arrows

[9] These three state descriptions of increased risk—marked with an asterisk (*) in latter data tables—identify a unique capability of STPA for 3S analysis. Namely, these three states are identified as conceptually similar (e.g., leading to the same set of high-level losses), meaning that the three different system requirements identified in Table 3 are interdependent.

[10] Identified by research team as important element of safeguards for the international transportation of SNF, that is currently not captured in related safeguards analysis techniques.

[11] *Ibid.*

[12] For example, more than XX minutes within XX meters of population or individual.

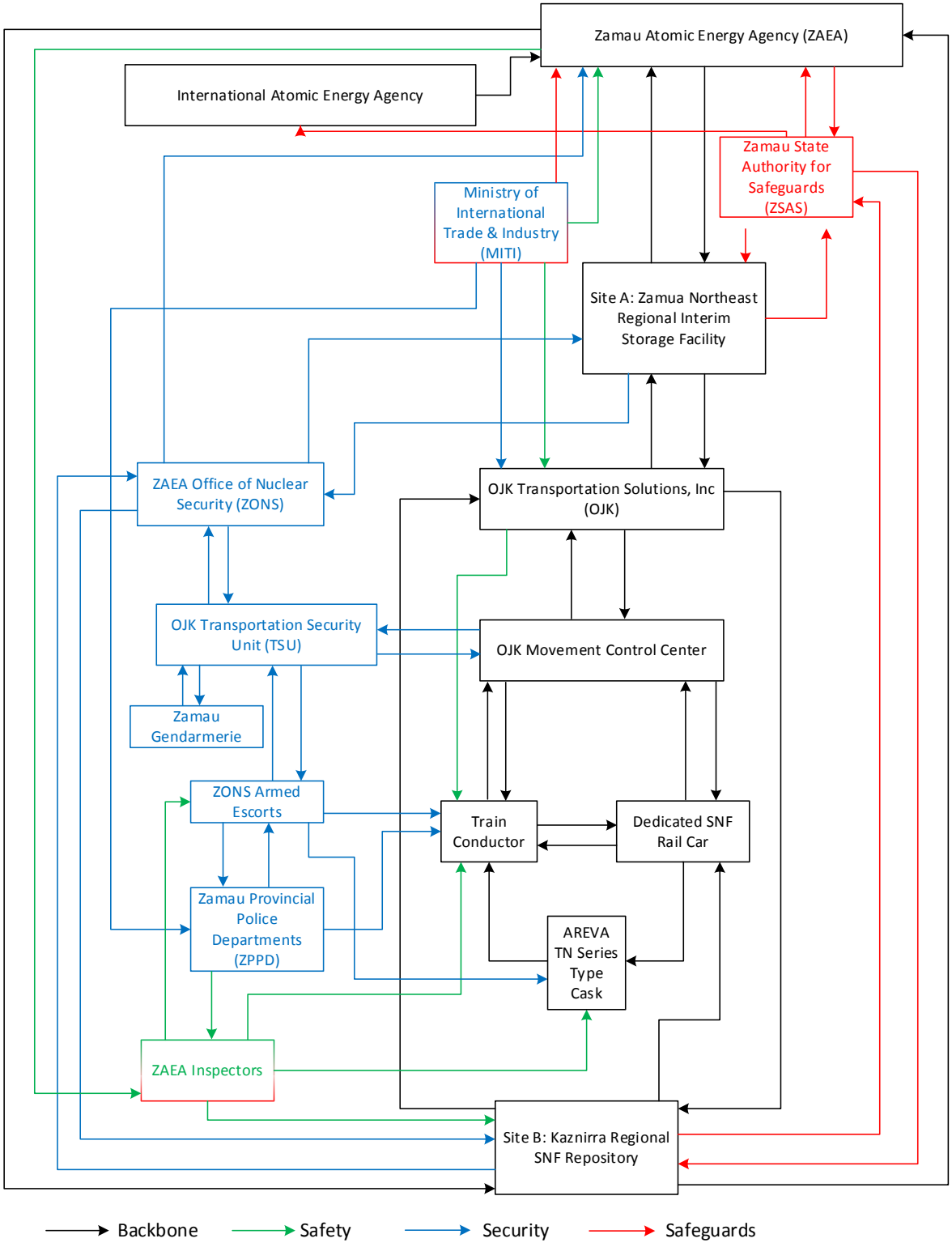

Figure 7. 3S Hierarchical Control Structure for STPA Analysis of Scenario 1.

represent feedback), STAMP identifies and describes these component-specific responsibilities in terms of higher-level control actions intended to bound emerging behaviors from lower hierarchical levels. As such, if the control action is successfully accomplished, emerging behaviors from lower hierarchical levels are constrained within desired limits and matriculate up through the HCS to result in desired system-level behaviors. The fourth column of Table 9 below lists a representative set of control actions.

Table 9. Representative Set of System Requirements and Associated Control Actions Necessary in Scenario 1 to Support System Requirements to Mitigate Related States of Increased Risk (and their Related Losses) for Safety, Security, and Safeguards of International SNF Transportation.

Emergent Property	State of Increased Risk	System Requirement	Representative Control Action [Specific Controller]
Safety	Unplanned radiological release from the cask*	All radiological release(s) from the cask must be planned and verified	Lid provides airtight seal [Cask]
			Physical assessment of cask contents conducted in appropriately sealed facility [Inspector]
	Transportation vehicle exceeds regulated speed limits	Transportation vehicle must always abide by posted, regulated speed limits	Throttle governor stops acceleration once at 55mph [Transportation Vehicle]
			Adhere to posted speed limits [Driver]
Security	Unauthorized access of cask*	Unauthorized individuals must not access the cask	Engage lid-locking mechanism [Cask]
			Check credentials of inspectors of the cask [Local Law Enforcement Agency]
	Unverified transfer of armed security responsibility	Any transfer of armed security must be verified	Confirm scheduled time for security responsibility transfer [Transportation Security Operations]
			Communicate process for transfer of armed security responsibilities [Competent Security Authority]
Safeguards	Loss of "continuity of knowledge" of SNF material status*	Accurate SNF material status must be maintained at all times	Transmit GPS location of SNF [Cask]
			Submit confirmation of physical inventory verification within 24 hours [Inspectors]
	Untimely reporting of SNF removal	All reporting of SNF removal must be reported with IAEA guidelines	Record manifest of SNF removed from inventory [Facility of Departure]
			Submit confirmation of removing SNF into inventory within 48 hours to IAEA [State Authority for Safeguards]

Evaluate How Control Actions Could Become Violated (describe how behavior of the sociotechnical system can violate the derived control actions necessary for desired system-level behaviors):

Colloquially known as "STPA: Step 1," each derived control action is evaluated to identify possible violations—from within the sociotechnical system model—that lead to system states of increased risk. Such system states of increased risk result when:

- Incorrect control actions are issued.
- Required control actions are not issued.
- Required control actions are provided too early, too late, or out of order.
- Required control actions are stopped too soon or engaged too long.

Each row within the STPA Step 1 tables consists of alternative system states, or possible states of the system predicated upon a specific violation of the related control action. Each cell within this row then represents an undesired end state—a state with increased risk—to be avoided though the enforcement of control actions. The STPA Step 1 data tables for Scenario 1 are provided in Appendix C. Table 10 shows the control actions evaluated for this analysis.

Table 10. Representative Set of Control Actions, with Both Traditional and 3S STPA Labels, Evaluated in Scenario 1 for International SNF Transportation.

Description	Control Action	Traditional STPA Label	3S Label
Representative Safeguards Control Action (Technical)	Transmit GPS location of SNF cask	SGCA1	3SCA1
Representative Safeguards Control Action (Social)	Submit confirmation of removing SNF from inventory within 48 hours to IAEA	SGCA2	3SCA2
Representative Safety Control Action (Social)	Physical assessment of cask contents in appropriately sealed facility	SACA1	3SCA3
Representative Safety Control Action (Technical)	Stop acceleration once at 55pmh	SACA2	3SCA4
Representative Security Control Action (Technical)	Engage rail car immobilization mechanism	SECA1	3SCA5
Representative Security Control Action (Social)	Communicate the process for transferring armed security responsibility	SECA2	3SCA6

Develop (Representative) Causal Scenarios (describe how real-world operation of the sociotechnical system can oppose completion of necessary control actions).

This is the traditional second broad step in STPA, but the lack of formalism, consistency, and rigor in its application render its inclusion beyond the scope of this analysis.

Table 11 summarizes the states of increased risk (SIR) resulting from the loss of control for the six representative control actions previously described.

Table 11. Summary of STPA Step 1 Results for the Six Representative Control Actions for Scenario 1.

Control action	STPA Label 3S STPA Label	SIR Identified
Transmit GPS location of SNF cask	SGCA1	SIR10 ($NNP_{1,2}$)
	3SCA1	SIR10, SIR12 ($NNP_{1,2}$)
Submit confirmation of removing SNF from inventory within 48 hours to IAEA	SGCA2	SIR10, SIR11 (NNP) SIR10 (PNN_2)
	3SCA2	SIR10, SIR11, SIR12 (NNP) SIR10, SIR12 (PNN_2)
Physical assessment of cask contents in appropriately sealed facility	SACA1	SIR1, SIR2 (NNP_2) SIR1, SIR2 ($PNN_{1,2}$)
	3SCA3	SIR12 (NNP_1) SIR1, SIR2 (NNP_2) SIR1, SIR2, SIR5, SIR7 ($PNN_{1,2}$)
Stop acceleration once at 55mph	SACA2	SIR4 (NNP_1)
	3SCA4	SIR4 (NNP_1) SIR8 (Too early)
Engage rail car immobilization mechanism	SECA1	SIR5, SIR6 (NNP) SIR5, SIR7 (PNN_1)
	3SCA5	SIR5, SIR6 (NNP) SIR5, SIR7 (PNN_1) SIR2 (PNN_2)
Communicate the process for transferring armed security responsibility	SECA2	SIR9 (NNP) SIR7, SIR9 (PNN_1)
	3SCA6	SIR5, SIR9, SIR10 (NNP) SIR5, SIR7, SIR9 (PNN_1)
NNP = "needed, not provided"; PNN = "provided, not needed"; Too early = "provided tool early" Subscripts denote a particular conditional description for a violated control action aligned with a given state of increased		

3.3. 3S Meta-Analysis

For this research thrust, the research evaluated the differences (if any) that emerged when evaluating "risk" in the international transportation of SNF with STPA using an integrated 3S approach. By comparing (Figure 8) the states of increased risk identified through both the "independent" safety, security, and safeguards STPA and the 3S STPA analysis provided in Table 11, gaps, interdependencies, conflicts and leverage points between safety, security, and safeguards were identified. Per the logic of STPA, the states of increased risk identified in the evaluation of each control action are conceptually equivalent; there is no distinction, prioritization, or bias to the relative importance of one state of increased risk over the other. This is helpful for this comparative analysis because a "hazardous" state for a safety control action, a "vulnerable" state for a security control action and a "proliferation" state for a safeguards control action are all conceptually equivalent to a state of increased risk resulting from the 3S STPA analysis.

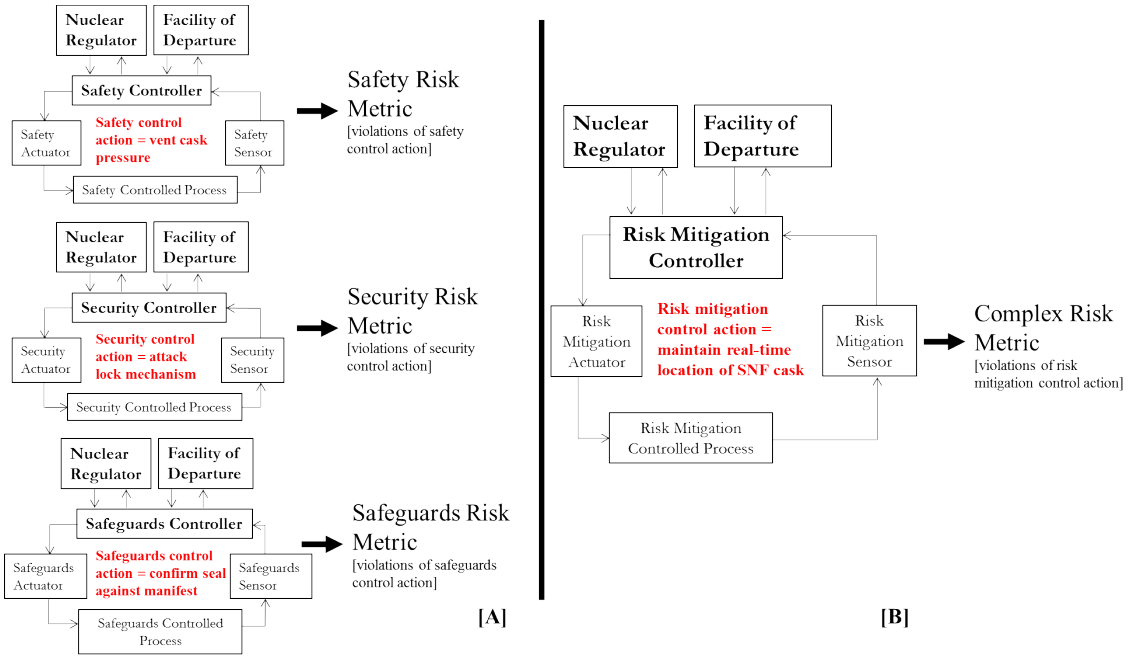

Figure 8. Comparative STPA Research Framework, via Representative Control Loops for Individual Characteristic (A) and 3S Complex Risk (B) STPA Analysis.

Comparing the states of increased risk listed in Table 11 shows two key trends. First, each 3S control action identified the same states of increased risk as their independent counterpart and identified additional states of increased risk associated with control action violations. Second, STPA's "provided, not needed" category of control action violation was the most common place where interdependence was illustrated. For example, for 3S control action 3 (a traditional safety control action), SIR5 and SIR7 (traditionally vulnerable states related to security control actions) were identified under the "provided, not needed" condition—states of increased risk missed when looking at SACA1 from an independent safety STPA lens. Other examples include 3S control actions 2, 5, and 6.

In addition to STPA's theoretical argument that violations of control actions lead to undesired system states that are conceptually similar, this analysis further suggested that the commonality across specific undesired states is evidence for the interdependence between safety, security, and safeguards. Consider the first row of Table 8, where the *unplanned radiological release from the cask*, *unauthorized access of cask*, and *loss of "continuity of knowledge" of SNF material status* each describe a similar state of the international SNF transportation system in which control over the cask is forfeited—and the same suite of losses are possible. In other words, even though a high-level security requirement is to prevent unauthorized access to the cask, a violated security control could *also* result in an unplanned radiological release (a safety hazard) or a loss of continuity of knowledge (a safeguards issue).

It is similarly interesting to note that this research also identified essential states of increased risk that do not fit directly under either safety, security, or safeguards, suggesting that they could be missed (at least in part, if not entirely) by independently analyzing these emergent properties. One such example is the uncoordinated implementation of operational concepts of operations across safety, security, and safeguards. For example, are the normal safety operations (or

expected operations) de-conflicted with the normal security operations (or expected operations). A second example considers the implementation of safety, security, and safeguards emergency plans. In the hypothetical international SNF scenario used in the analysis, conflicts quickly emerged when thinking through responsibilities for the various controllers in response to the train derailment, interactive effects that were not captured in the independent STPA analyses. This introduces the importance of considering such "3S-based states of increased risk."

Lastly, the process of constructing the HCS (for both the independent and 3S analyses) was instructive in highlighting gaps, interdependencies, conflicts, and leverage points between safety, security, and safeguards. With the HCS as a complex system model, safety, security, or safeguards gaps quickly and clearly emerge when identifying the needed presence of control and feedback channels to support high-level requirements. Likewise, conflicts and leverage points are indicated also where either (1) a single controller has multiple incoming control actions to process, which oftentimes are not aligned; (2) a single controller has multiple outgoing control actions to send; or (3) multiple controllers receive the same control action for execution. More specifically, caution should be taken when controllers have control actions related to multiple emergent properties (the inspectors with safety and safeguards responsibilities in the 3S HCS in Figure 7, for example). Such synergies *can be* exploited to enhance operational efficiency (or, in other words, reduce costs) in risk-mitigation measures: consider the assignment of basic safeguards inspection responsibilities to a safety regulatory inspector in a country with limited resources. However, these types of *interdependencies* can easily overload, distract, or bias controllers against completing each set of responsibilities accurately, timely, and comprehensively.

Taken together, these insights suggest that STPA (1) better incorporates multi-faceted interactions in complex risk facing international SNF transportation and (2) offers a useful framework to understand and manage the growing risk complexity within (and across) other NFC activities in dynamic 21st century environments.

4. COMPLEX RISK

Drawing on complexity and systems theories, this research addressed gaps in understanding risk complexity in the NFC with the development of a new conceptualization of risk, referred to as "complex risk." In the case of the international transportation spent nuclear fuel, complex risk is a term that encompasses—and, therefore, is not limited to any one of the—traditional definitions of risk associated with security, safety, and safeguards. However, unlike many traditional engineering approaches to risk, complex risk also accounts for the social, political, and technical contexts that produce the pressures and dynamics that prevent the completion of the desired system objectives. In addition to incorporating the broader contexts for risk, complex risk accounts for the emergence of risk resulting from interactions among security, safety, and safeguards risks and mitigations.

4.1. Explanation

Incorporating complexity and systems theories into engineering risk helps bridge the gap between traditional risk analysis techniques and the operational reality of risk management. This research showed that risk is not just the probabilistic calculation of technical components reliably completing designed functions, but must describe how social dynamics influence resultant behaviors. Our goal was not to precisely define risk, but rather to introduce a new concept with characteristics derived from complexity and systems theories:

- **Interdependence** explains how social influences can alter the ability of technical components to complete desired functions.
- **Emergence** explains how system-level behavior can result from interactions among social and technical components.
- **Hierarchy** asserts that higher ranking components/influences constrain the emerging behaviors of components/influences at lower levels.

These insights informed a novel approach to visualize complex risk as a "state space." Here, all possible system states can be described by total state space (T). There is some subset of this total state space that represents all desirable system states (D); thus, the space (T-D) is the undesirable, or "risky," space. All else being equal, being in the desirable space minimizes risk, establishing the system objective of staying within the desirable space. Given this system objective, complex risk can be understood conceptually as a function of the distance from the current state within the desirable space to the nearest boundary and the speed at which forces are pulling/pushing the system toward the boundary of the desirable space.

Because the requirements that define the desirable space are implemented in different social, political, and technical contexts, a system may exist at different places in the desirable space at different points in time. Figure 9 depicts the position of a system within the desirable space at two different time intervals, Node A and Node B. The system depicted in Figure 9(a) is relatively desirable because both Node A and Node B are centrally located within the desirable space (i.e., they are relatively far from the system boundary). However, complex risk is dynamic and involves not only a point estimate of risk but also all system states between the two points, as in Figure 9(b). While the system may appear to have relatively low risk at Nodes A and B, Figure 9(b) depicts how there are multiples points that approach the boundary of the desirable space.

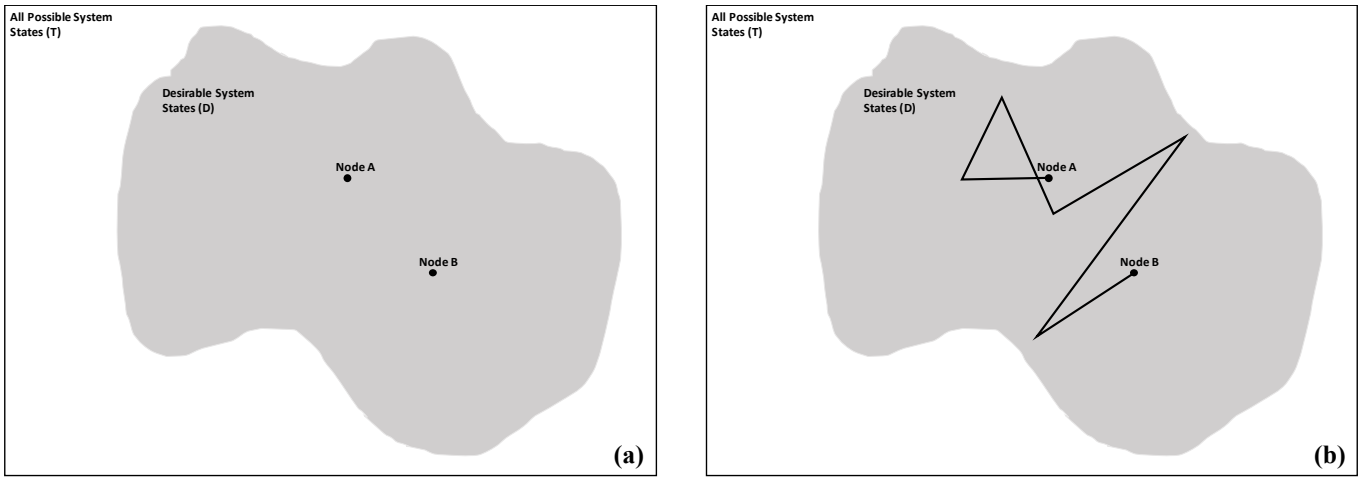

Figure 9. Static (a) and Dynamic (b) State Space Visualizations of Complex Risk.

4.2. Position within the Risk Literature Landscape

Exploring how risk is conceptualized across various academic disciplines—ranging from engineering to organization science to cognitive psychology—provided an opportunity to compare various approaches to risk definition, quantification, assessment, and management. This comparison highlighted the need for a broader conceptualization of risk to fully account for, and in turn manage, the complexity of risks facing NFC activities (a representative sample is provided in Table 12), and resulting from international SNF transportation specifically. Such a conceptualization must address the two key gaps. First, it should be data-pluralistic, helping to avoid the limitations of purely probabilistic approaches to risk assessment. Second, it should be systems-oriented framework, thereby avoiding the limitations of micro-macro extrapolation [38].

For more, see the detailed literature review (and summary) provided in "Exploring Risk Complexity: A Risk Literature Survey & Review (SAND2017-TBD)," [39].

Table 12. Summary of Approaches to Risk from Multiple Academic Disciplines.

Name [ref] (Emphasis[13])	Summary	Advantages	Disadvantages	Analytical Gaps[14]
"Set of Triplets" [40] (Risk Definition)	• Probability *and* consequence over a given set of scenarios: Risk = $\{(s_i, p_i, x_i)\}$, i=1,2 ,..., N+1	• First-level definition is computationally simple and visually accessible via risk tables or risk curves. • Accounts for multi-dimensionality of consequences and incomplete information . • Definition used by NRC [17].	• Requires comparability in measures of consequence. • Acknowledges subjectivity in probability assessment, but does not incorporate social-psychological elements of risk.	• Limited data plurality, unclear how to incorporate qualitative measures. • Presumably could be applied to each "S" in isolation (assuming data could be standardized within analysis), but does not provide for interaction/feedback.
Systems-Based Principles for Risk [41] (Risk Analysis, Management & Communication)	• Develops a set of 10 common principles of risk grounded in systems engineering. • Defines risk as probability of an event and probability of the severity of an event.	• Clearly articulates how to systems theory informs (and, possibly, unites) risk analysis. • Positions these principles within a broader risk analysis approach, graphically depicted as a "roadmap."	• Application case (NextGen) is useful for demonstrating how the advocated principles are relevant, but is not sufficiently detailed to provide legibility into how each principle might be operationalized.	• Theoretically, many of the principles are consistent with the 3S approach, although additional work is needed to translate the process as applied to NextGen to the SNF context; much of the article is on the *"what"* not the *"how"*.
Knightian & Bayesian Approaches to Risk [42] (Risk Analysis)	• Defines a risk decision as "a stochastic optimization problem where the parameters and functional forms required to determine optional decisions are known."	• Resolves Knightian and Bayesian approaches to risk (objective risk, subjective risk, or uncertainty, statistical risk) using complexity theory.	• Although resolving theoretical differences, the implications for the practice of risk assessment are not clear, particularly outside of the field of industrial organization.	• Provides useful framework for thinking about decision-making under uncertainty, but it's unclear how this framework may apply to the SNF context broadly and to integrated 3S analysis specifically.
Complexity Based Risk Evaluation [43] (Risk Analysis)	• Defines complexity as "degree of difficulty in accurately predicting future behavior."	• Provides a method to move from a broad "reference definition" of complexity to specific metrics using system, observer, and behavior entropy models and presents an application case.	• Requires considerable existing data/expertise about various sources of risk. • Focuses mostly on the uncertainty aspect of risk (identifying causes of deviation from a system state).	• Provides a framework for disaggregating rather than aggregating risk sources and metrics. • Does not address the interactions among risks.

[13] Options: Risk definition (quantitative, qualitative, both), risk management, risk analysis and risk communication.
[14] Only analytical gaps vis-à-vis 3S analysis of SNF international transportation included.

Name [ref] (Emphasis[13])	Summary	Advantages	Disadvantages	Analytical Gaps[14]
Characterizing Risk by Coupling and Tractability [44] (Risk Analysis)	• Describes risk analysis as an exercise in imagining what can go wrong (and how), this involves understanding the problem and the mechanism that gave way to the problem.	• Acknowledges that different types of systems require different methods of risk analysis. • Draws on Perrow's (1984) dimensions of accidents, interactive-ness and coupling, to develop a typology of various systems and risks.	• Provides a very broad definition of risk: adverse outcome in some present/future state. • Does not consider the potential mismatch between tools and data, nor address how multiple tools might be integrated.	• Safety (and presumably security by extension) is defined as the absence of the adverse outcome rather than as some desired state. • Provides an approach for selection among risk analysis approaches, which we've already done, but not carrying out integrated risk assessment.
Complexity Theory & the Management of Risk [45] (Risk Management)	• Risk is emergent, rather than mechanistic and as such risk managers should view organizations as ecologies, not machines.	• Provides a framework for using complexity theory for risk management in complex systems. • Identifies the factors that cause complex systems to "drift" into failure or success.	• Does not provide a definition of risk not an actionable framework for risk analysis nor address issues related to data plurality.	• Proposes a solution—diversity—which may not be feasible in the 3S context given the relative lack of centralized control and repeat players.

4.3. Results from Hypothetical International SNF Transportation Analysis

A complex risk evaluation of the hypothetical SNF transportation case resulted in necessary tradeoffs as each hypothetical country simultaneously considered resource allocation for meeting high-level safety, security, and safeguards performance requirements along the entire route. Figure 10 visualizes the 3S complex risk profiles for three implementation scenarios.

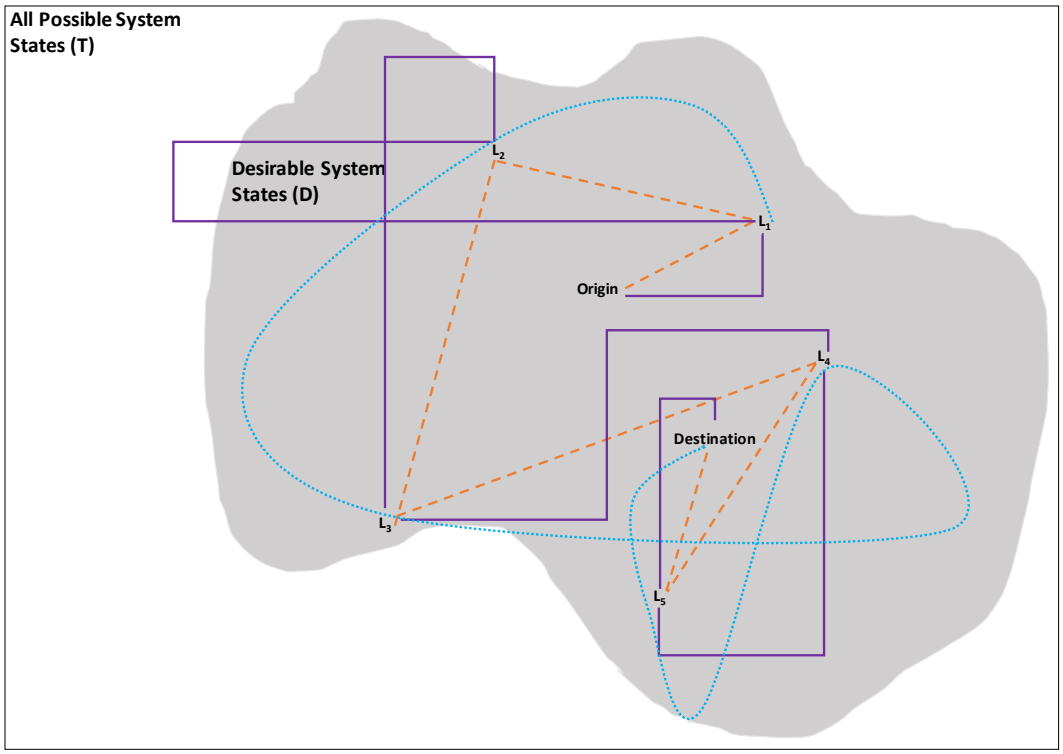

Figure 10. 3S Implementation Tradeoffs for Three Possible Implementation Scenarios for a Hypothetical SNF Transportation Case.

More specifically, the orange scenario represents the most optimal tradeoffs in implementing safety, security, and safeguards requirements and therefore has the lowest 3S risk, as depicted by its relative centrality and the minimal spread of its risk profile. The purple scenario represents moderate tradeoffs and resulting 3S risk. The blue scenario represents the least-optimal tradeoffs in implementing safety, security, and safeguards requirements and therefore has the highest 3S risk, as depicted by the spread of its risk profile and crossing outside the desirable state.

4.4. Implications

Conceptually, complex risk is a function of the distance from the current state within the desirable space to the nearest boundary and the speed at which forces are pulling/pushing the system toward the boundary of the desirable space (i.e., the system objective). Operationally, complex risk are those pressures and dynamics that prevent completion of the objective (i.e., the operational objective). Building on key theoretical concepts, complex risk provides a new perspective to understand and analyze the complexity of operational realities.

This application of the complex risk concept to the SNF transportation case speaks to the utility of the concept, and for understanding and managing risk in the NFC more broadly. First, this

application case distinguished sources of risk that can be controlled (i.e., defining and implementing high-level requirements) from those that cannot (i.e., external events and inherent risk associated with various modes). Second, this application case enabled the identification of aspects of the route that have considerable risk variability because of implementation with those that are relatively high-risk, regardless of implementation. Furthermore, it underscored the value of understanding risk as not only a probabilistic calculation of technical components reliably functioning, but also a result of the interaction of technical components and social dynamics.

For more, see [38] and [46].

5. CONCLUSIONS

Evaluating a hypothetical case description and scenario for international SNF transportation, both grounded in operational realities and accepted by a diverse panel of relevant SMEs, provided rich data sets with which to evaluate risk complexity in the NFC and address three main research goals.

First, generating the hypothetical case description (Section1.3.2) and scenario (1.3.3) provided a deeper understanding of systemic threats and risks related to international SNF transportation, whether stemming from technical or socio-political sources. Often, these risks are addressed through the independent lenses of safety, security, and safeguards, making the process of understanding risk complexity akin to finding equivalencies between apples, Volvos, and sunsets. Better understanding real-world risk facing international SNF transportation, however, helped identify gaps (e.g., the potential for there to be no single entity responsible for overseeing the entirety of the SNF shipment), interdependencies (e.g., the need to coordinate between secondary security responders and emergency personnel after Scenario 1's notional train derailment), conflicts (e.g., SNF cask inspectors who have both safety and safeguards responsibilities), and leverage points (e.g., using security responsibility handover procedures as additional checks on SNF location to maintain "continuity of knowledge") across traditional safety, security, and safeguards approaches. These relationships aided in identifying systematic frameworks by which to develop 3S frameworks. Despite the inherent limitations in purely mathematical representations of risk, this research found that the new system state-based concept (Section 4) is a helpful start for managing risk complexity in NFC activities.

Second, employing two novel, system-theoretic analysis techniques helped to develop international SNF transportation risk assessment frameworks. Again, these risk assessment frameworks were developed to match the real-world complexity (often mitigated by simplifying assumptions in traditional approaches) provided in the hypothetical case study and scenario generation (for more details, please see [14]). In addition, this research demonstrated insights from applying DPRA to account for three disparate risk assessment perspectives by extending the ADAPT software to link three disparate software codes (Section 2). More specifically, the ability to branch through various possibilities in the scenario better accounts for both epistemic and aleatory uncertainty present in risk complexity, especially when looking at the interactions between safety, security, and safeguards. This research similarly demonstrated an extension of STPA to account for these three disparate risk assessment perspectives in a single analysis. The resulting hierarchical control structure model of international SNF transportation (Figure 7) illustrates how risk can emerge from individual failures, interactive failures, or interactions between correctly accomplished tasks.

Third, comparing the outcomes of the independent risk assessments with the outcomes of the integrated 3S risk assessments provided a mechanism by which to evaluate the effectiveness of the using DPRA and STPA as complex risk assessment frameworks. First, the ability for both DPRA and STPA to include more complexity (e.g., uncertainty) provided more accurate socio-technical system models to evaluate. Second, comparing the outcomes of independent "S" analysis versus integrated 3S analysis yielded interesting insights in both DPRA (Figure 5) and STPA (Figure 8) thrusts, including how including interdependencies (and their cumulative consequence-related effects) better aligns with real-world operational uncertainties and modeling multi-level interactions better describes the complexity associated with multi-model, multi-

jurisdictional systems. Third, these results indicate that risk mitigation strategies resulting from integrated 3S risk assessments can be designed to better account for interdependencies not included in independent "S" assessments. Here, the new state-based construct of "complex risk" is instructive by changing the paradigm from risk minimization to risk management in a complex, dynamic, and interactive tradespace.

5.1. Implications

The results of this research indicate that interdependent risks (1) are inherent in NFC activities and (2) can go unidentified when each "S" is independently evaluated. As such, efforts to reduce global nuclear dangers related to the proliferation of NFC activities should include a mechanism for identifying and mitigating these interdependencies. This research also illustrated that system-theoretic analysis techniques better capture "real-world" complexity for NFC activities than traditional approaches. Here, DPRA and STPA are viable candidates for new risk management approaches aimed at addressing various types of risk complexity expected with evolving and growing international NFC activities.

The parallel research thrusts also demonstrated that both DPRA and STPA can be extended into novel application spaces. This research serves as both the first use of DPRA to conceptually translate between three disparate perceptions of risk and of ADAPT to link three distinct software codes. Although just a proof-of-concept, the successful generation of results implies that DPRA could be explored for a more robust, quantitative approach to characterizing integrated 3S interactions and risk complexity. Likewise, this research is the first use of STPA to account for three separate emergent properties of complex systems, also implying its potential use as the basis for a more rigorous risk management framework. Other results from this research include the first known application to international nuclear safeguards and indications of a conceptual and analytical relationship between STPA and network theory [47] that provides a mechanism by which to prioritize states of increased risk resulting from identifying possible control action violations.

Lastly, this research supports an argument that risk *itself* can be complex, as well as existing in complex environments [46] [38]. This offers a (potentially substantial) paradigm shift in risk assessment and risk management for NFC activities as risk is understood from the inside out as a dynamic balance within a system state-based tradespace. Such a state-based description is well suited to help navigate the increasing risk complexity in NFC activities and, in conjunction with DPRA and/or STPA, provide the foundation for new, more robust, and more comprehensive risk management frameworks.

The interdependency between nuclear safety, security, and safeguards supported by this research suggests a need—and provides a way—to reprioritize U.S. Government engagement efforts to reduce global nuclear risks. Although just scratching the surface, these results offer a better understanding of 3S interactions that can help design nuclear facilities, systems, and activities (especially those in new nuclear countries) more capable of managing complex risks. As this is one of the first rigorous, technical evaluations of 3S analysis, the results of this research put DPRA, STPA, their respective extensions developed at Sandia and this state-based construct of complex risk at the forefront of the discussion to streamline nuclear operations across safety, security, and safeguards mission areas.

5.2. Limitations

Although compelling, there are a few limitations to the insights, conclusions, and implications of this research. First, the reliance on a hypothetical case for analysis inherently limits the generalizability of the insights. Further, despite the efforts taken to ground the hypothetical case description in real data and real-world experiences across a range of related SMEs, the inability to directly link insights to real-world occurrences limits the utility of these insights. Another limitation stems from the use of a single case research design. Evaluating only one scenario of concern limits the robustness of the results and insights. This limitation, however, is somewhat mitigated by applying two separate analysis techniques to the same case study. Lastly, the increased complication of linking software codes based on different scripting languages, coding languages, operating systems, and hardware platforms prevented establishing the "clean" connections hypothesized at the outset of this project.

5.3. Future Work

Although this LDRD research built on experience Sandia gained from past related studies (for example, [5], [6], [7], and [8]), the rigorous approach described in this report can be the foundation for a series of additional research efforts. First, to account for the limitation discussed in the previous section, by leveraging ongoing work at another part of the laboratories, Sandia has begun (and will continue) to collect "real data" on the international transportation of an SNF cask. Doing so provides real data against which to benchmark (and, if needed, improve the fidelity of) the hypothetical case description and an opportunity to evaluate a second SNF transportation-related case. Similarly, this same research design could be applied to other NFC activities, including (but not limited to) geological repositories, advanced nuclear reactor technologies, or with nuclear power plant builds in new nuclear countries.

Additionally, this complex risk paradigm and set of system-theoretic frameworks could be applied to other ongoing research efforts at Sandia, including (but not limited to) investigating possible expansions to traditional probabilistic risk assessment approaches to better understand risks associated between safety and security in NFC activities[15] and providing analytical insights for understanding risks in a

> more holistic and integrated approach to understanding how trends and decisions might play out across the nuclear policy and technology space with a Global Nuclear Enterprise framework.[16]

The complex risk paradigm offers both of these projects a new perspective for framing their respective issues. Similarly, both DPRA and STPA provide novel techniques with which to generate the necessary analytical insights for these two projects to be successful.

Methodologically, the results of this research suggest three areas where Sandia can spearhead technical advances. The first is the need to more deeply explore the complex risk paradigm. This could include—but should not be limited to—investigating the benefits and challenges to quantified and mathematical descriptions of complex risk, assessing alternative visualization options for the complex risk tradespace, and exploring the use of basic physics statics

[15] As initiated by an August 2017 multi-lab, multi-stakeholder "Extended Probabilistic Risk Assessment (ePRA)" Workshop hosted at Sandia-Livermore and summarized in a forthcoming SAND report.
[16] This research project is being summarized in the forthcoming, "Global Nuclear Enterprise FY17 System Study" SAND Report. Note: This SAND report is marked 'Official Use Only.'

(e.g., balance of forces) and dynamics (e.g., potential energy wells or unstable energy equilibria) concepts as metaphors in the complex risk tradespace.

Second, consistent with other Sandia programs[17], this research introduces where to begin additional efforts to expand the analytical capabilities for DPRA, to include—but not be limited to—developing software scripts to automate links between disparate codes, creating the process to rigorously develop "translation tables" (e.g., the edit and branching rules) correlating inputs and outputs between disparate software codes, and generating new techniques for evaluating the quantified uncertainty resulting from simulating three disparate codes.

Third, these research results identify areas in which Sandia could expand the usability of STPA, including—but not limited to—exploring new techniques for organizing and prioritizing violated control actions (either in combination with currently known techniques or developing new techniques), or developing rigorous frameworks for using STPA in applications where intentionality plays a larger conceptual role (than in STPA's legacy of system safety) in causing systems to enter undesired states.

Lastly, future work also includes the potential for *combining* DPRA and STPA, enabling the logical prioritization of the former leverage the robust scenario generation of the latter, similar to current work at Sandia exploring "STPA-Informed Fault Tree Analysis" [48].

[17] For example, LDRD 191054 "Nuclear Power Plant Cyber Security Discrete Dynamic Event Tree Analysis" Project and the DOE/Office of Nuclear Energy-funded "The Progress and Insights from Severe Accident Analysis Modeling for Severe Accident Management Guidelines" Project.

REFERENCES

[1] O. Heinonen, "Nuclear Terrorism: Renewed Thinking for a Changing Landscape," 13 February 2017. [Online]. Available: http://www.defenddemocracy.org/media-hit/olli-heinonen1-nuclear-terrorism-renewed-thinking-for-a-changing-landscape/. [Accessed 18 September 2017].

[2] H. A. Munera, M. B. Canal and M. Munoz, "Risk associated with transportation of spent nuclear fuel under demanding security constraints: The Colombian experience," *Risk Analysis,* vol. 17, no. 3, pp. 381-389, 1997.

[3] A. Khlopkiv and A. Lutkova, "The Bushehr NPP: Why Did It Take So Long?," *Center for Energy and Security Studies,* 2010.

[4] World Institute for Nuclear Security, "Nuclear Transport Security: International Best Practice Guide," WINS, Vienna, Austria, 2014.

[5] R. Ghanbari and A. Doll, "Safety, Security and Safeguards Integration into U.S. Nuclear Power Plants (SAND2010-6007P)," Sandia National Laboratories, Albuquerque, NM, 2010-Unpublished.

[6] A. Mohagheghi, "Education Programs for Integrated Nuclear Safeguards, Safety, and Security (Invited Talk)," in *IAEA Conference on Managing the Development of a Sustainable National Infrastructure for Nuclear Power Plants*, Vienna, Austria, 2012.

[7] F. Ghanbari and A. D. Williams, "A Systems Approach for Developing an Integrated Nuclear Safety, Safeguards and Security ('3S') Framework (SAND2013-0964P, 0889P)," Sandia National Laboratories, Albuquerque, NM, 2012-Unpublished.

[8] J. Darby, K. Horak, J. LaChance, K. Tolk and D. Whitehead, "Integrating Safety, Operations, Security and Safeguards (ISOSS) Into the Design and Operation of Nuclear Facilities (SAND2007-6429)," Sandia National Laboratories, Albuquerque, NM, 2007.

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

[10] A. Cipollaro and G. Lomonaco, "Contributing to the Nuclear 3S's Via a Methodology Aiming at Enhancing the Synergies Between Nuclear Security and Safety," *Progess on Nuclear Energy,* no. 86, pp. 31-39, 2016.

[11] E. Garbolino, J. Chery and F. Guarnieri, "A Simplified Approach to Risk Assessment Based on System Dynamics: An Industrial Case Study," *Risk Analysis,* vol. 36, no. 1, pp. 16-29, 2016.

[12] R. K. Yin, Case Study Research: Design and Methods, 5th ed., Los Angeles, CA: Sage, 2013.

[13] K. M. Eisenhardt, "Building Theories from Case Study Research," *Academy of Management Review,* vol. 14, no. 4, pp. 532-550, 1989.

[14] A. D. Williams, D. Osborn, K. A. Jones, E. A. Kalinina, B. Cohn, M. Thomas, M. J. Parks, E. Parks and A. H. Mohagheghi, "Hypothetical Case and Scenario Description for International Transportation of Spent Nuclear Fuel (SAND2017-TBD)," Sandia National Laboratories, Albuquerque, NM, 2017.

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

[16] Office of Civilian Radioactive Waste Management, U.S. Department of Energy, "FINAL-Environmental Impact Statement for a Geological Repository for the Disposal of Spent Nuclear Fuel and High-Level Radioactive Waste at Yucca Mountain, Nye County, Nevada (DOE/EIS-0250)," U.S. Department of Energy, Washington, D.C., 2002.

[17] U.S. Nuclear Regulatory Commission, "Spent Nuclear Fuel Transportation Risk Assessment-Final Report (NUREG-2125)," U.S. Nuclear Regulatory Commission, Washington, D.C., 2014.

[18] D. Dominguez, M. Parks, A. Williams and S. Washburn, "Special Nuclear Material and Critical Infrastructure Security Modeling and Simulation of Physical Protection Systems," in *IEEE International Carnahan Conference on Security Technology*, Boston, MA, 2012.

[19] B. Cipit and M. J. Parks, "Integration of Materials Accountancy and Process Monitoring Data with Physical Protection," in *IAEA Conference on Nuclear Security*, Vienna, Austria, 2016.

[20] M. Yue, L.-Y. Cheng and R. A. Bari, "A Markov Model Approach to Proliferation-Resistance Assessment of Nuclear Energy Systems," *Nuclear Technology,* vol. 162, no. 1, pp. 26-44, 2008.

[21] S. Mladineo, R. Denning, J. Roglans-Ribas, R. Bari, J. Eagle, J. Olinger, J. Phillips, G. Rochau, R. Schock and S. McGuire, "Guidelines for the Performance of Nonproliferation Assessments (PNNL-14294)," Pacific Northwest National Laboratory, Richland, WA, 2003.

[22] M. Thomas, A. D. Williams, D. M. Osborn, K. A. Jones, E. A. Kalinina, M. J. Parks and A. H. Mohagheghi, "An Integrated 3S Model for Safeguards for International Transport of Spent Nuclear Fuel," in *Proceedings of the ESARDA 39th Annual Meeting*, Dusseldorf, Germany, 2017.

[23] N. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety, Cambridge, MA: MIT Press, 2012.

[24] N. Leveson, N. Dulac, D. Zipkin, J. Cutcher-Gershenfeld, J. Carroll and B. Barrett, "Engineering resilience into safety-critical systems," *Resilience Engineering--Concepts and Precepts,* pp. 95-123, 2006.

[25] A. D. Williams, "System Security: Rethinking Security for Facilities with Nuclear Materials," *Transactions of the American Nuclear Society,* vol. 109, no. 1, pp. 1946-1947, 2013.

[26] C. H. Fleming and N. G. Leveson, "Improving Hazard Analysis and Certification of Integrated Modular Avionics," *Journal of Aerospace Information Systems,* vol. 11, no. 6, 2014.

[27] T. Ishmatsu, N. G. Leveson, J. Thomas, J. Fleming, M. Katahira, y. Miyamoto, R. Ujiie, H. Nakao and N. Hoshino, "Hazard Analysis of Complex Spacecraft using Systems Theoretic Process Analysis," *AIAA Journal of Spacecraft and Rockets,* vol. 51, no. 2, pp. 509-522, 2014.

[28] S. Placke, J. Thomas and D. Suo, "Integration of Multiple Active Safety Systems Using STPA SAE Technical Paper 2015-01-0277," SAE, 2015.

[29] M. V. Stringfellow, N. G. Leveson and B. D. Owens, "Safety-driven design for software-intensive areospace and automotive systems," in *Proceedings of the Insitute of Electrical and Electronics Engineers (IEEE)*, 2010.

[30] H. Alemzadeh, J. Raman, N. Leveson and K. I. Ravishankar, "'Safety Implications of

Robotic Surgery: A Study of 13 Years of Data on Da Vinci Surgical Systems Coordinated Science Laboratory Report (UILU-ENG-13-2208)," University of Illinois at Urbana-Champaign, Urbana-Champaign, 2013.

[31] T. Pawlicki, A. Samost, D. Brown, R. Manger, G.-Y. Kim and N. Leveson, "Application of Systems and Control Theory-Based Hazard Analysis to Radiation Oncology," *Journal of Medical Physics,* vol. 43, no. 3, pp. 1514-1530, 2016.

[32] J. Thomas, F. Luiz de Lemos and N. Leveson, "Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants Research Report NRC-HQ-11-6-04-0060," Massachusetts Institute of Technology, Cambridge, MA, 2012.

[33] Electric Power Research Institute, "Hazard Analysis Methods for Digital Instrumentation and Control Systems Technical Report 3002000509," Electric Power Research Institute, 2013.

[34] J. R. Laracy and N. G. Leveson, "Applying STAMP to Critical Infrastructure Protection," in *IEEE Conferece on Technologies for Homeland Security*, 2007.

[35] W. Young and N. Leveson, "An Integrated Approach to Safety and Security Based on Systems Theory," *Communications of the ACM,* vol. 57, no. 2, pp. 31-35, 2014.

[36] W. Young, "A System-Theoretic Security Analysis Methodology for Assuring Complex Operations Against Cyber Disruptions," Massachussets Institute of Technology, Dissertation, Cambridge, MA, 2015.

[37] A. D. Williams, "Beyond a Series of Security Nets: Applying STAMP & STPA to Port Security," *Journal of Transportation Security,* vol. 8, no. 3-4, pp. 139-157, 2015.

[38] A. D. Williams and M. DeMenno, "A New Approach for Addressing Risk Complexity in the Nuclear Fuel Cycle," *Risk Analysis,* 2017-Submitted.

[39] A. D. Williams, M. DeMenno and A. Macherla, "Exploring Risk Complexity: A Risk Literature Survey & Review (SAND2017-TBD)," Sandia National Laboratories, Albuquerque, NM, 2017.

[40] S. Kaplan and J. B. Garrick, "On The Quantitative Definition of Risk," *Risk Analysis,* vol. 1, no. 1, pp. 11-27, 1981.

[41] Y. Y. Haimes, "Systems-Based Guiding Principles for Risk Modeling, Planning, Assessment, Management, and Communication," *Risk Analysis,* vol. 32, no. 9, pp. 1451-1467, 2012.

[42] A. L. Norman and D. W. Shimer, "Risk, uncertainty, and complexity," *Journal of Economic Dynamics and Control,* vol. 18, pp. 231-249, 1994.

[43] J. Fischi and R. Nichiani, "Complexity based risk evaluation in engineered systems," *Procedia Computer Science,* vol. 44, pp. 31-41, 2015.

[44] E. Hollnagel, "The changing nature of risk," *Ergonomics Australia Journal,* vol. 22, no. 1-2, pp. 33-46, 2008.

[45] S. W. A. Dekker, "Drifting into failure: Complexity theory and the management of risk," in *Chaos and Complexity Theory for Management: Nonlinear Dynamics*, Hershey, PA: IGI Global Business Science Reference, 2013, pp. 241-253.

[46] A. D. Williams and M. DeMenno, "Toward a New Approach to Risk Complexity in the Nuclear Fuel Cycle," in *Proceeedings of the 58th INMM Annual Meeting*, Palm Desert, CA, 2017.

[47] A. D. Williams and K. A. Jones, "Invoking Network & System Theory to Improve Security Risk Management in International Spent Nuclear Fuel Transportation," in *Proceeedings of*

the 58th INMM Annual Meeting, Palm Desert, CA, 2017.

[48] A. J. Clark, A. D. Williams and T. A. Wheeler, "Addressing Cyber Hazards in Nuclear Power Plants with STPA-Informed Fault Tree Analysis," *International Journal of Safety Science ,* 2017-in press.

[49] M. Bell, "ORIGEN-the ORNL Isotope Generation and Depletion Code," 1973.

[50] U.S. Nuclear Regulatory Commission, "State-of-the-Art Reactor Consequence Analysis (SOARCA) Project (NUREG-1935)," U.S. Nuclear Regulatory Commission, Washington, D.C., 2012.

[51] M. Abkowitz and E. Bickford, "Development of Rail Accident Rates for Spent Nuclear Fuel Rail Shipments," in *International High Level Radioactive Waste Management Conference*, Phoenix, AZ, 2017.

APPENDIX A: PROJECT BIBLIOGRAPHY

Conference Papers

A. D. Williams, D. Osborn, R. Homan, K. A. Jones, E. A. Kalinina and A. H. Mohagheghi, "Preliminary Results from a System-Theoretic Framework for Mitigating Complex Risks in International Transport of Spent Nuclear Fuel," in *Proceedings of the INMM 57th Annual Meeting*, Atlanta, 2016.

A. D. Williams, D. M. Osborn, K. A. Jones, B. Cohn, M. J. Parks, E. Parks, E. S. Johnson and A. H. Mohagheghi, "A New Look at Transportation Security: A Complex Risk Mitigation Framework for the Security of International Spent Nuclear Fuel Transportation," in *IAEA Conference on Nuclear Security*, Vienna, Austria, 2016.

A. D. Williams, K. A. Jones, D. Osborn, E. A. Kalinina, A. H. Mohagheghi and M. J. Parks, "Investigating a System-Theoretic Framework for Mitigating," in *Poster for the Annual Meeting of the Society for Risk Analysis*, San Diego, CA, 2016.

E. A. Kalinina, B. Cohn, D. Osborn, A. D. Williams, M. J. Parks, K. A. Jones, N. Andrews, E. Johnson, E. Parks and A. H. Mohagheghi, "Example of Integration of Safety and Security Using Dynamic Probabilistic Risk Assessment under A System-Theoretic Framework," in *Proceedings of the IHLRWMC*, Charlotte, NC, 2017.

M. Thomas, A. D. Williams, D. M. Osborn, K. A. Jones, E. A. Kalinina, M. J. Parks and A. H. Mohagheghi, "An Integrated 3S Model for Safeguards for International Transport of Spent Nuclear Fuel," in *Proceedings of the ESARDA 39th Annual Meeting*, Dusseldorf, Germany, 2017.

A. D. Williams, D. Osborn, K. A. Jones, E. A. Kalinina, B. Cohn, M. J. Parks, E. Parks, B. Jeantete, M. A. Thomas and A. H. Mohagheghi, "Intermediate Results from a System-Theoretic Framework for Mitigating Complex Risks in International Transport of Spent Nuclear Fuel," in *Proceedings of the 58th INMM Annual Meeting*, Palm Desert, CA, 2017.

A. D. Williams and M. DeMenno, "Toward a New Approach to Risk Complexity in the Nuclear Fuel Cycle," in *Proceedings of the 58th INMM Annual Meeting*, Palm Desert, CA, 2017.

A. D. Williams and K. A. Jones, "Invoking Network & System Theory to Improve Security Risk Management in International Spent Nuclear Fuel Transportation," in *Proceedings of the 58th INMM Annual Meeting*, Palm Desert, CA, 2017.

A. D. Williams, "Improvements in Transportation Security Analysis from a Complex Risk Mitigation Framework for the Security of International Spent Nuclear Fuel Transportation," in *IAEA Conference on Physical Protection of Nuclear Material and Nuclear Facilities*, Vienna, Austria, 2017.

SAND Reports

A. D. Williams, D. Osborn, K. A. Jones, E. A. Kalinina, B. Cohn, A. H. 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: FINAL REPORT (SAND2017-TBD)," Sandia National Laboratories, Albuquerque, NM, 2017.

A. D. Williams, D. Osborn, K. A. Jones, E. A. Kalinina, B. Cohn, M. Thomas, M. J. Parks, E. Parks and A. H. Mohagheghi, " Hypothetical Case and Scenario Description for International Transportation of Spent Nuclear Fuel (SAND2017-TBD)," Sandia National Laboratories, Albuquerque, NM, 2017.

A. D. Williams, M. DeMenno and A. Macherla, "Exploring Risk Complexity: A Risk Literature Survey & Review (SAND2017-TBD)," Sandia National Laboratories, Albuquerque, NM, 2017.

Journal Articles

A. D. Williams, M. DeMenno and G. Wyss, "A New Approach for Addressing Risk Complexity in the Nuclear Fuel Cycle," *Risk Analysis*, 2017-Submitted.

A. D. Williams and K. A. Jones, "Applying STPA to Explore Safety, Security & Safeguards (3S) Interactions in International Spent Nuclear Fuel Transportation," *Reliability Engineering & System Safety*, 2017-In preparation.

B. Cohn, A. D. Williams and D. M. Osborn, "Extending DPRA to Evaluate Safety, Security & Safeguards in International Spent Nuclear Fuel Transportation," *Reliability Engineering & System Safety*, 2017-Pending.

Invited Presentations

Extended Probabilistic Risk Assessment (ePRA) Workshop (August 2017, Livermore, CA)

- SAND2017-7514C

Sandia Risk Team Information Exchange (August 2016, Albuquerque, NM)

- SAND2016-7085C

Center for Strategic and International Studies' Nuclear Energy Experts Group

- SAND2016-7085C (September 2016, Singapore)
- SAND2017-3572C (February 2017, Singapore)

Briefings to various guests and dignitary visits to the Center for Global Security and Cooperation

- NA22
- NA24
- International collaborators

APPENDIX B: DPRA DOCUMENTATION

RADTRAN Data: Scenario 1

Scenario Description

The scenario evaluated by RADTRAN assumes that an accident or attack of a certain severity occurs at some location along the land transportation route. The accident/attack results in release of a fraction of radionuclide inventory of the transportation cask content into the environment and its dispersion in the air. The water routes are not considered because dispersion associated with release into oceans or other bodies of water is not modeled in RADTRAN. People downwind from the accident/attack location are exposed to external radiation emitted by airborne particulates and particulates deposited on the ground and to internal radiation via inhalation.

RADTRAN simulates the atmospheric dispersion using a Gaussian plume model for a "puff" release, which is an instantaneous spherical release (Figure 1). The Gaussian plume equation is modified to include particulate deposition. This model assumes:

- The predominant force in plume transport is the wind; i.e., gases, aerosols, and particles dispersed in the air move predominantly downwind.
- Dispersion is assumed to occur from a point or small area source.
- The greatest concentration of material in a plume is along the plume centerline.
- Aerosols, gases, and other materials in a plume diffuse spontaneously from regions of higher concentration to regions of lower concentration.

In Gaussian models for a "puff" release (i.e., for an idealized instantaneous, perfectly spherical release), the concentration of the material in the puff has a normal distribution along the two axes perpendicular to wind direction (Figure 11). Note that practical minimum distance for applying the Gaussian model is about 20 meters from the release source.

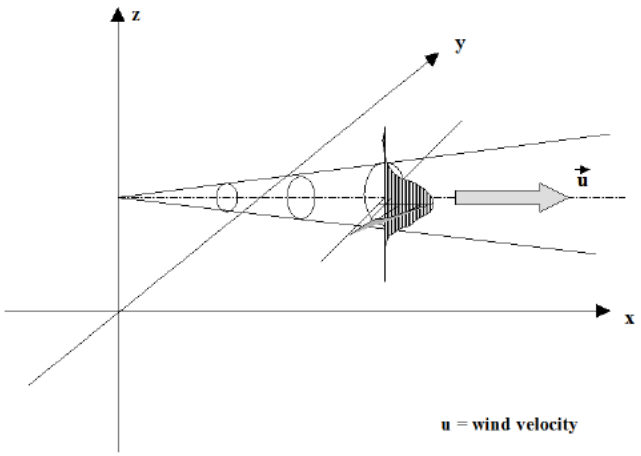

Figure 11. Gaussian Plume Diagram (from RADTRAN technical manual).

Input Parameters

Radionuclide Inventory – supplied in 24 RADTRAN input files

The radionuclide inventory of a spent fuel assembly is a function of fuel type (PWR or BWR), age (time from discharge), and burnup. The calculations for a typical PWR and a typical BWR assembly were done with ORIGEN [49]. Twelve combinations of three burnups (40, 50, and 60 GWD) and four ages (5, 10, 25, and 50 years) were considered for a PWR and a BWR assembly.

The transportation cask is either a generic PWR cask with 24 assemblies or a generic BWR cask with 52 assemblies [14]. The inventory of the PWR cask is the inventory of the PWR assembly times 24. The inventory of the BWR cask is the inventory of the BWR assembly times 52.

Note that each PWR/BWR assembly has more than 200 radionuclides. Not all radionuclides were included in the cask inventory, only those considered in NUREG-2125 [17] and the Yucca Mountain environmental impact statement [16], and any additional radionuclides (if present) that contribute to >90% of the human health effects (e.g., 69 SOARCA radionuclides) [50]. The included radionuclides constitute 94.4–99.8% of the total activity, depending on the fuel type and case. Table 13 and Table 14 provide PWR and BWR transportation cask inventories for each of 12 cases.

Each radionuclide is also assigned to one of four physical groups (Table 13 and Table 14) because this information is required for RADTRAN (different physical groups may behave differently when dispersed).

In spent nuclear fuel, a mixture of actinides and fission products are gases, volatile materials, CRUD (a generic term for corrosion and wear products (rust particles, etc.) that become radioactive (i.e., activated) when exposed to radiation), and solid particulate matter. The radionuclides assigned to the same group exhibit similar physical and chemical properties. These properties are deposition velocity, fraction of each nuclide that becomes airborne, and the fraction of such airborne material that is respirable.

The information in Table 13 and Table 14 is used by ADAPT to specify the RADTRAN input parameters corresponding to the scenario in consideration.

Release Fractions

Each accident/attack scenario has associated release fractions for each group of radionuclides in the transportation cask inventory. It is assumed that the transportation cask and spent fuel assemblies in the cask are damaged in the accident/attack and some fraction of the radionuclide inventory is released from the fuel rods into the cask and from the cask into the environment, where it is dispersed in the air.

The following is required for the RADTRAN input file:

- Total release fraction (the release fraction from rods to cask times the release fraction from cask to the environment).
- The fraction of the total release that is aerosol. The common assumption is that all the released particles are aerosolized (aerosol fraction is equal to 1).
- The fraction of the aerosol release that is respirable (10 microns aerodynamic diameter).

The aerosolized material (InventoryxRelease FractionxAerolized fraction) is the source of external exposure. The respirable material (Aerolized MaterilalxRespirable fraction) is the source of exposure via inhalation, including inhalation of re-suspended material.

The above fractions have to be specified for each physical group. An example of release fractions for a severe accident (NUREG-2125) and for a hypothetical attack is shown in Table 15. The release fractions for a severe accident with uncanistered PWR (NUREG-2125) are shown in Table 15 in parentheses. For this example, it was hypothesized that if the cask and SNF are damaged in an attack, the release fractions of particles and volatiles from rods to cask would be 50 times higher than in accident scenarios considered in NUREG-2125. It was assumed that the release fractions of CRUD and gas would be the same as in NUREG-2125 accidents. It was further assumed that 100% of gases released in the cask would be released into the environment. The same values as NUREG-2125 were assumed for the aerosol and respirable fractions for chemical/physical forms. The scenario-specific release fractions will be supplied by ADAPT. The release fractions may not necessarily fall within the range used for the above example.

Source Dimensions – Fixed and Same for PWR and BWR Casks

The following are the dimensions of the generic PWR and BWR transportation casks (and are the same in all scenarios):

- Cask height (source height): 5.1 m
- Cask radius (source width): 1.2 m

Heat Flux

The source heat was set to 0.13 cal/s[18] in all the scenarios.

Release Height

The release height depends on whether the cask remains on the transportation vehicle or is dropped to the ground as a result of an accident/attack. The release height was 2 m in all scenarios. This assumes that the cask remains on the rail car.

Dispersion Parameters

The dispersion parameters depend on the weather conditions at the location and time of an accident/attack. Consequently, these parameters are supplied by ADAPT. The following dispersion parameters need to be defined:

- Wind speed (m/s)
- Anemometer height (m) – the height at which the wind is measured, commonly 10 m
- Ambient temperature (0K)
- Atmospheric mixing height (m)
- Atmospheric stability class
- Rainfall (mm/hour) – only light rainfall can be modeled

[18] This is the same value as in NUREG-2125.

The information in Table 16 can be used to select the appropriate atmospheric stability class. All parameters listed above were the same in all the scenarios, except the wind speed.

Deposition Velocity

The deposition velocity is defined for each physical group. The deposition velocity of gas is equal to 0 and thus is fixed. The deposition velocity for volatile, particles, and CRUD is defined via ADAPT. Note that the values of deposition velocity that RADTRAN accommodates are between 0.0–0.1 m/sec. The same deposition velocities were used in all the scenarios.

Exposure Parameters

The following are the exposure parameters:

- Evacuation time
- Breathing rate (m^3/s)
- Resuspension half-life
- Acceptable contamination level (population can return after 50 years)
- Duration of cleanup (if any)
- Interdiction level after clean up

These parameters have to be specified outside RADTRAN and passed on to the RADTRAN input file.

The default evacuation time in RADTRAN is 1 day (24 hours). The default breathing rate in RADTRAN is 3.3E-04 m^3/s. The acceptable soil contamination (as proposed in EPA guideline) is 0.2 Bq/m^2 for total deposited activity. The suggested interdiction level is 40 times the acceptable contamination level (default value). The default resuspension half-life is 15 days. (Note that many exposure parameters—radionuclide dose conversion factors—are defined in the RADTRAN library.)

All parameters listed above were the same in all the scenarios, except the evacuation time.

Consequence Analysis

The probability of an accident/attack is set equal to 1 in all scenarios. This allows for calculating doses, not consequence. The consequences are calculated outside RADTRAN based on the probability of the accident/attack of specific severity.

RADTRAN calculates doses for the following pathways:

- Inhalation
- Cloudshine
- Resuspension
- Groundshine
- Ingestion

Note that the ingestion dose calculated by RADTRAN is not used. The ingestion dose model assumes that every radioactive atom is ingested by someone and therefore contributes to a collective, societal dose.

The following consequence-related parameters can be calculated: dose to the maximally exposed individual (MEI) during evacuation.

- Number of early fatalities.
- Activity of the soil within the contaminant plume at the time of release.
- Area of interdicted land.
- Cost of cleanup.

The primary output used by ADAPT is maximum exposed individual (MEI).

Isotope	Class*	Burnup 60				Burnup 50				Burnup 40			
		5yr	10yr	25yr	50yr	5yr	10yr	25yr	50yr	5yr	10yr	25yr	50yr
am241	4	12468.32	20484.97	35148.32	43619.03	12151.78	19879.78	34013.84	42174.49	10869.41	17782.05	30424.22	37724.11
am242	4	71.35784	69.62595	64.68	57.20497	74.29622	72.49297	67.3427	59.56216	67.00541	65.3773	60.73362	53.71395
am242m	4	71.68865	69.94378	64.97514	57.46768	74.64	72.83027	67.65405	59.83589	67.31027	65.67568	61.01254	53.96108
am243	4	670.2486	669.9243	668.9514	667.3946	424.1189	423.9178	423.3211	422.3286	222.6357	222.5319	222.2205	221.6951
ce144	4	114214.1	1347.308	0.002211	5.05E-13	117853	1390.184	0.002282	5.21E-13	119344.9	1407.762	0.002311	5.28E-13
cm243	4	396.8951	352.3654	246.5578	135.9827	275.5005	244.5859	171.1459	94.39135	149.1178	132.3892	92.63351	51.09016
cm244	4	147120	121511.4	68464.86	26313.08	70378.38	58128.65	32750.92	12587.68	26434.38	21832.86	12300.97	4727.741
co 60	3	11904.65	6170.919	859.5892	32.17232	9718.054	5037.665	701.7081	26.26443	7624.865	3952.605	550.5665	20.60692
cs134	2	740886.5	138493	904.5405	0.206432	552136.2	103206.5	674.0757	0.153834	378259.5	70702.7	461.7989	0.105386
cs137	2	1840670	1640497	1161341	653059.5	1549686	1381103	977708.1	549781.6	1252476	1116259	790183.8	444343.8
eu154	4	86309.19	57701.19	17239.78	2302.119	72181.62	48252.97	14417.51	1925.189	54531.24	36456	10892.11	1454.53
eu155	4	39121.3	18877.62	2121.081	55.49319	31724.76	15308.76	1720.022	45.00065	23178.16	11184.65	1256.692	32.87805
kr 85	1	130144.9	94313.51	35896.22	7175.351	117645.4	85258.38	32449.95	6486.227	101798.9	73770.81	28078.05	5612.432
pu238	4	89429.19	85965.41	76371.89	62693.84	64120.22	61641.08	54760.86	44957.84	39586.38	38056.86	33810.16	27760.86
pu239	4	2536.411	2536.216	2535.503	2534.335	2621.903	2621.643	2620.8	2619.308	2697.341	2696.951	2695.914	2694.227
pu240	4	5443.914	5511.697	5649.341	5750.595	4966.249	4997.449	5059.524	5101.751	4248.389	4258.768	4278.357	4287.957
pu241	4	1146357	899610.8	434802.2	129437.8	1105168	867308.1	419189.2	124780.5	988540.5	775783.8	374951.4	111606.5
pu242	4	54.55719	54.55654	54.55589	54.55459	37.05016	37.05016	37.04951	37.04886	22.00086	22.00086	22.00086	22.00022
ru106	4	221448.6	7371.892	0.271933	1.11E-08	182588.1	6078.097	0.224212	9.17E-09	143597.8	4780.281	0.176335	7.21E-09
sb125	4	39970.38	11388.97	263.4486	0.49477	34038.49	9698.595	224.3546	0.421343	27867.89	7940.108	183.6843	0.344958
sr 90	4	1259935	1117168	778702.7	426720	1125211	997621.6	695416.2	381074.6	961686.5	852648.6	594356.8	325699.5
te125m	4	9787.459	2788.8	64.51135	0.121155	8335.135	2374.897	54.9373	0.103174	6823.784	1944.389	44.97795	0.084467
u234	4	11.73016	12.96714	16.39784	21.28541	13.88303	14.76973	17.23005	20.73405	16.27784	16.8253	18.34378	20.50703
y 90	4	1260259	1117427	778897.3	426830.3	1125470	997881.1	695610.8	381171.9	961945.9	852908.1	594505.9	325783.8
ba137m	2	1743114	1553514	1099784	618415.1	1467503	1307935	925881.1	520644.3	1186054	1057103	748345.9	420791.4
cm242	4	427.7643	57.87373	53.49016	47.30854	369.4054	60.22573	55.69492	49.25773	270.8562	54.2867	50.22616	44.42141
np239	4	670.2486	669.9243	668.9514	667.3946	424.1189	423.9178	423.3211	422.3286	222.6357	222.5319	222.2205	221.6951
pr144	4	114220.5	1347.308	0.002211	5.05E-13	117859.5	1390.249	0.002282	5.21E-13	119351.4	1407.827	0.002311	5.28E-13
pr144m	4	1090.573	12.864	2.11E-05	4.82E-15	1125.276	13.2733	2.18E-05	4.98E-15	1139.546	13.4413	2.21E-05	5.04E-15
rh106	4	221448.6	7371.892	0.271933	1.11E-08	182588.1	6078.097	0.224212	9.17E-09	143597.8	4780.281	0.176335	7.21E-09
te127	4	0.485397	4.42E-06	3.35E-21	0	0.492564	4.49E-06	3.4E-21	0	0.496839	0	3.43E-21	0
te127m	4	0.495555	4.52E-06	3.42E-21	0	0.502871	4.58E-06	3.47E-21	0	0.507243	4.62E-06	3.5E-21	0
TOTAL		**9240255**	**6913368**	**4500885**	**2406648**	**7956764**	**5984555**	**3894517**	**2074543**	**6562693**	**4958473**	**3228071**	**1713230**

Table 13. PWR Cask Activity in Curies (24 Assemblies).

***Class:** 1 = Volatile, 2 = CRUD, 3 = Particulate, 4 = Volatile

Table 14. BWR Cask Activity in Curies (52 Assemblies).

Isotope	Class*	Burnup 60				Burnup 50				Burnup 40			
		5yr	10yr	25yr	50yr	5yr	10yr	25yr	50yr	5yr	10yr	25yr	50yr
am241	4	12579.08	20247.68	34269.41	42353.3	11597.41	18663.78	31583.68	39032.32	9753.654	15770.05	26772.97	33118.38
am242	4	69.25135	67.57189	62.77103	55.51632	63.99654	62.44357	58.0067	51.30292	50.98811	49.75135	46.21676	40.87622
am242m	4	69.57038	67.88249	63.06054	55.77211	64.29027	62.73027	58.27373	51.53903	51.22281	49.98043	46.43038	41.06314
am243	4	554.9946	554.7276	553.9546	552.6476	331.5914	331.4368	330.973	330.2	164.067	163.9968	163.7578	163.3784
ce144	4	78638.05	927.5957	0.001522	3.48E-13	81728.54	964.0659	0.001582	3.61E-13	84178.16	992.947	0.00163	3.72E-13
cm243	4	345.1957	306.4627	214.4508	118.2691	224.4714	199.2865	139.4457	76.90519	115.7295	102.7436	71.89351	39.6507
cm244	4	93449.62	77183.46	43486.05	16713.08	43931.57	36283.35	20443.03	7857.059	16090.49	13289.94	7487.859	2877.849
co 60	3	22130.92	11472.04	1597.946	59.80984	18790.27	9740.303	1356.736	50.78151	15338.59	7951.222	1107.544	41.45384
cs134	2	493114.6	92176.32	602.0335	0.13739	372629.2	69653.3	454.9297	0.103819	260126.5	48624.22	317.5795	0.072475
cs137	2	1433092	1277176	904139.5	508405.4	1209689	1078115	763219.5	429168.6	980059.5	873473.5	618350.3	347697.3
eu154	4	70146.59	46895.57	14011.47	1871.016	57665.19	38550.27	11518.28	1538.076	42541.62	28439.78	8497.362	1134.696
eu155	4	32502.81	15684.32	1762.238	46.10432	26033.73	12562.64	1411.589	36.92843	18769.19	9057.276	1017.668	26.624
kr 85	1	97161.3	70412.22	26799.68	5356.843	88384.54	64051.35	24378.16	4872.962	77083.68	55862.05	21260.97	4249.805
pu238	4	64903.03	62394.38	55427.78	45505.62	45401.62	43646.27	38775.14	31835.24	27538.92	26475.03	23522.27	19313.08
pu239	4	2757.968	2757.686	2756.843	2755.297	2837.232	2836.951	2835.968	2834.141	2878.832	2878.411	2877.286	2875.459
pu240	4	6351.168	6392.768	6475.546	6532.324	5631.741	5650.011	5684.724	5704.4	4650.205	4655.405	4664.119	4664.541
pu241	4	1097355	861162.2	416210.8	123896.3	1011147	793520	383521.1	114156.9	860853	675564.3	326503.8	97186.59
pu242	4	39.08995	39.08995	39.08854	39.08854	26.68443	26.68443	26.68443	26.68303	15.97665	15.97665	15.97665	15.97665
ru106	4	159260.5	5301.33	0.195562	7.99E-09	135701.7	4517.395	0.166639	6.81E-09	110664.4	3683.849	0.135894	5.56E-09
sb125	4	29156.54	8307.632	192.1751	0.360908	25436.43	7247.676	167.6508	0.314867	21311.57	6072.335	140.4689	0.263809
sr 90	4	963152.4	853980.5	595259.5	326194.6	860276.8	762769.7	531678.9	291354.6	736797.8	653274.6	455365.4	249543.8
te125m	4	7139.6	2034.324	47.05859	0.088378	6228.757	1774.746	41.0547	0.077101	5218.551	1486.919	34.39589	0.064598
u234	4	10.50203	11.39981	13.88976	17.43686	11.94187	12.56966	14.31124	16.79319	13.57411	13.95497	15.01114	16.51632
y 90	4	963391.4	854191.4	595414.1	326278.9	860487.6	762966.5	531819.5	291424.9	736980.5	653443.2	455491.9	249600
ba137m	2	1357059	1209478	856215.1	481449.7	1145560	1020971	722771.9	406415.1	928101.6	827165.4	585562.2	329272.4
cm242	4	404.1805	56.16	51.91146	45.91178	323.96	51.87773	47.97211	42.42778	220.733	41.31751	38.22141	33.80422
np239	4	554.9946	554.7276	553.9546	552.6476	331.5914	331.4368	330.973	330.2	164.067	163.9968	163.7578	163.3784
pr144	4	78640.86	927.6378	0.001522	3.48E-13	81731.35	964.0941	0.001582	3.61E-13	84180.97	992.9751	0.00163	3.72E-13
pr144m	4	750.8378	8.856724	1.45E-05	3.32E-15	780.3373	9.204843	1.51E-05	3.45E-15	803.7232	9.480584	1.56E-05	3.55E-15
rh106	4	159260.5	5301.33	0.195562	7.99E-09	135701.7	4517.395	0.166639	6.81E-09	110665.8	3683.849	0.135894	5.56E-09
te127	4	0	3.94E-06	2.98E-21	0	0.432977	3.95E-06	2.99E-21	0	0.429871	3.92E-06	2.97E-21	0
te127m	4	0.44089	4.02E-06	3.04E-21	0	0.442042	4.03E-06	3.05E-21	0	0.43888	4E-06	3.03E-21	0
TOTAL		**7224042**	**5486071**	**3556221**	**1888856**	**6228751**	**4741053**	**3072669**	**1627209**	**5135385**	**3913449**	**2539536**	**1342117**

***Class:** 1 = Volatile, 2 = CRUD, 3 = Particulate, 4 = Volatile

Table 15. Release Fractions Assumed for a Medium Consequences Attack.

Group	Release Fraction		Total Release Fraction	Aerosol Fraction	Respirable Fraction	Total Respirable
	Rods to Cask	Cask to Environment				
Gas	0.12	1 (0.8)	0.12 (0.096)	1	1	0.12 (0.096)
CRUD	1 (1)	0.001 (0.001)	0.001 (0.0101)	1 (1)	0.05 (0.05)	$5.0*10^{-5}$ ($5*10^{-5}$)
Particle	$1.68*10^{-4}$ ($4.8*10^{-6}$)	1 (0.7)	$1.68*10^{-4}$ ($3.36*10^{-6}$)	1 (1)	0.05 (0.05)	$8.4*10^{-6}$ ($1.68*10^{-7}$)
Volatile	$7.50*10^{-4}$ ($3.0*10^{-5}$)	1 (0.5)	$7.5*10^{-4}$ ($1.5*10^{-5}$)	1 (1)	0.05 (0.05)	$3.75*10^{-5}$ ($7.5*10^{-7}$)
NOTE: The values considered in NUREG-2125 for a severe accident are shown in parenthesis						

Table 16. Pasquill Stability Classes as Related to Solar Radiation and Wind Speed (Table 3-1 in RADTAN technical manual).

Surface wind speed at 10 m (m/sec)	DAY			NIGHT	
	Incoming Solar Radiation			Cloud Cover	
	Strong	Moderate	Slight	Overcast	Clear
<2	A	A-B	B	E	F
2-3	A-B	B	C	E	F
3-5	B	B-C	C	D	E
5-6	C	C-D	D	D	D
>6	C	D	D	D	D

STAGE Data: Scenario 1

Description of Scenario

The safety scenario will focus on the derailment of a transport vehicle and the subsequent adversarial attack that would compromise the transported spent nuclear fuel. It is assumed the transport vehicle (in this case rail) will be manned by a certain amount of response forces and vehicle operators. The amount of adversaries will be based on whether this scenario is a planned event or an opportunistic opportunity to "loot" a seemingly defenseless target. The scenario will determine the timeline from train departure to adversarial attack to attack response.

Input Parameters

STAGE has six distinct editors that simplify tasks to build, run, and control a scenario. This includes the Database Editor, Scenario Editor, Runtime Environment, Script Editor, Mission Editor, and Arinc424Editor. Input parameters are supplied in the Database Editor, Scripting Editor, and Mission Editor.

Database Editor

Profiles are set up that describe the properties of a specific object that can be added to a STAGE tactical environment (Figure 12). Within each profile are platforms that can function independently at runtime. Profiles include specific entities and parameters for each entity.

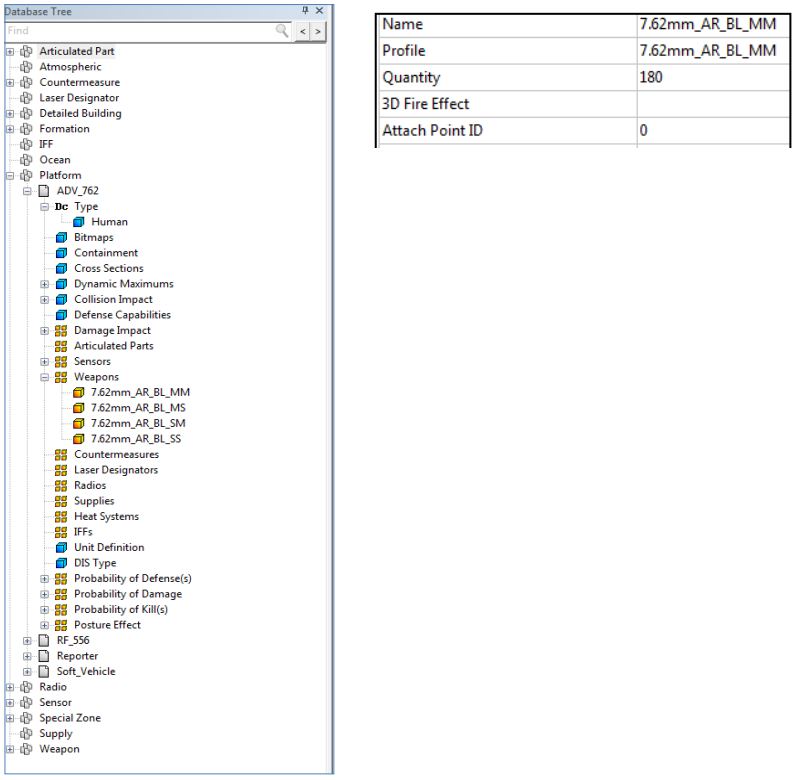

Figure 12. Profile, Platform, and Entity Set Up (Response/Adversary Numbers and Weapons).

Scenario Editor

The Scenario Editor allows entities to be added/removed, missions to be assigned, waypoints to be placed, and terrain to be specified (Figure 13). This is where the majority of STAGE development takes place.

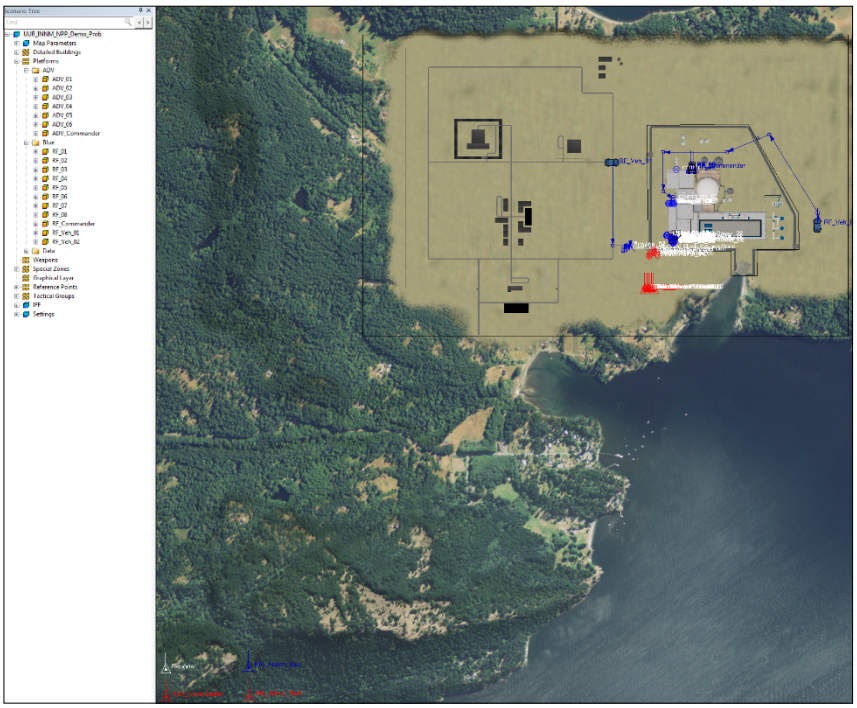

Figure 13. Entity Set Up (Scenario Editor).

Mission Editor

The Mission Editor enables the analyst to build, execute, monitor, and control missions that can be assigned to entities to control their behavior in a scenario (Figure 14).

Task Group	Type	Logical Oper.	Left Term	Oper.	Right Term	Action
Init	INIT					int Objective1Count=0 int Objective2Count=0
Task Group	AT		EXTERN EVENT	=	Disembark	Mission Start-RF_01
		AND	Reason	=		Wait-1s-Disembarked
		AND	From	=	RF_Vehicle_01	
Task Group1	AT		ACTION ENDED	=	Wait	Mission Start-RF_02
		AND	Ending State	=	COMPLETED	
		AND	Reason	=	Disembarked	
Task Group2	AT		TIME	=	00:00:05	Mission Start-RF_03 Mission Start-RF_04
Task Group3	AT		EXTERN EVENT	=	Reached Objective 1	Objective1Count++
		AND	Reason	=		Report Objective 1
		AND	From	=		
Task Group4	IF		Group Count-Inside Group Count	=	Objective1Count	Send Move to objective 2 TO TEAM
Task Group5	AT		EXTERN EVENT	=	Send Reached Objective 2	Objective2Count++
		AND	Reason	=		Report Objective 2
		AND	From	=		
Task Group6	IF		Group Count-Inside Group Count	=	Objective2Count	Send Move to objective 3 TO TEAM
End	END					

Figure 14. Entity Behavioral Set Up (Mission Editor).

Script Editor

The Script Editor allows for scripts to be written, using a pre-defined behavior language that is used to control an entity at runtime. Behaviors can be scripted prior to ingestion into scenario manager and runtime environment.

Runtime Environment

Once all parameters are established, the scenario will be executed via the Runtime Environment in STAGE. The following indicators will be analyzed:

- Detection – Time to detect adversaries:
  - Response force's ability to quickly assess the situation.
  - Overcoming potential impediments, such as line-of-sight limitations and potential injuries due to derailment.
- Delay – Time to slow down adversaries:
  - Employ barriers to immediately secure SNF shipment.
  - Evaluate train route and map out potential barriers (ravines, fences), or impediments to response forces (trees, hills).
- Response – Time to engage the adversary:
  - Assess injuries to response forces (25%, 50%, or 75%).
  - Remaining response forces available to activate weapons to stop or slow down attack.
  - Determine response/adversarial hits and kills.
  - Result: Response containment or adversarial theft.

STAGE Outputs

Each scenario run will be executed through a batch process. Ph/Pk tables will be used to determine the number of hits and kills for the response and adversarial forces. A Monte Carlo script will be applied to generate a random sampling for each run. In addition, the analyses will assess train damage and, in the case of a theft, which materials were taken and the damage to the existing SNF load.

Ph/Pk Definitions

- Effectiveness = Ph and the probability that a hit will kill a target at specified range.
- Ph/Pk data populates curve sets (Figure 15).
- A curve defines the Ph/Pk data for a munition-target pairing at discrete ranges for shooter/target state.
- Combining the shooter-target states of moving/stationary and standing/crouching/prone.
- Simulator linearly interpolates between range/probability values.

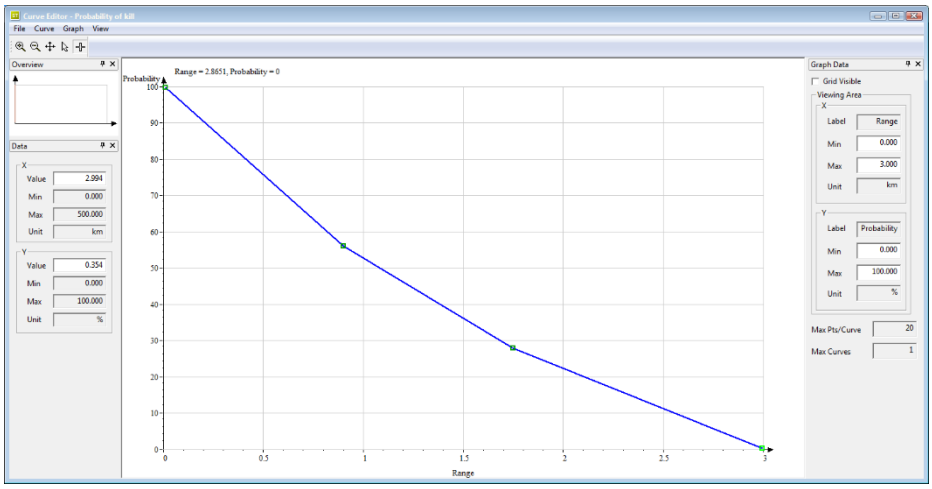

Figure 15. Ph/Pk Values.

Monte Carlo Methods

- Execute scripts to apply computational algorithms that perform random sampling to obtain numerical results.
  - Define a domain of possible inputs.
  - Generate inputs randomly from a probability distribution over the domain.
  - Perform a deterministic computation on the inputs.
  - Aggregate the results.
- Report on the overall outcomes of a specified number of scenarios.

Reports

- Generate reports with run results to determine overall outcomes.

Integration into 3S Framework

STAGE can be configured and controlled through ADAPT via initialization files. These files include database, scenario, platform, and mission files.

- Database files (.xml)
  - Hold references to static descriptors of scenario objects such as:
    - Entity types
    - Weapon types
    - Etc.
  - All scenarios within an analysis reference the same database.

- Scenario files (.scenario)
  - XML format.
  - Reference platform files for each entity.
  - Holds descriptions of the scenario as a whole such as:
    - Terrain
    - Buildings
    - Bitmaps
    - Waypoints
    - Special zones
- Platform files (.ptf)
  - XML format.
  - One for each entity in each scenario.
  - Holds entity specifics such as:
    - Location
    - Side
    - Mission
    - Etc.
  - ADAPT can update these files to match each branch.
- Mission files (.me_mission)
  - XML format.
  - Describe the entity behavior and artificial intelligence.
  - Mission files are referenced in the platform files and may be updates via ADAPT.

Command Line Capabilities

The Simulation Engine can be run from the command line with the commands in Figure 16.

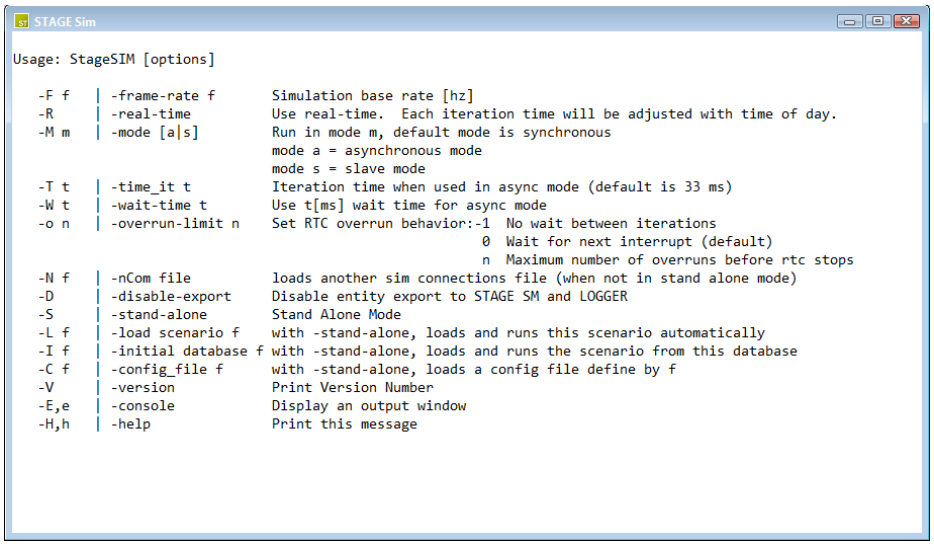

Figure 16. Command Line Options for Linking with ADAPT.

Through the -L and -I commands, the Simulation Engine can be given the scenario and database files to use. Logic must be configured within the scenario to signal to outside processes that the scenario is complete. Upon completion, ADAPT can read the output and branch according by updating the previously used scenario, platform, and mission files.

Linux

The documentation states that the Simulation Engine run in Linux, but this functionality has not yet been tested. Further research is required to determine if the necessary, non-standard STAGE plugins will work on Linux.

Entity Set Up

The integration of Scenario 1 (Figure 17) into the STAGE interface requires a numerical value for response and adversarial forces, as well as the weapons/materials available to each entity. Specific parameters are required for the train, including speed and payload. The scenario includes an inevitable train derailment, adversarial attack (theft), and possible response. Each entity parameter will be established under a specific profile and platform. Once parameters are established a scenario is set up through parameters in the Database Editor, visually in the Scenario Editor (graphic placement), and methodically in the Mission Editor (behavioral set up).

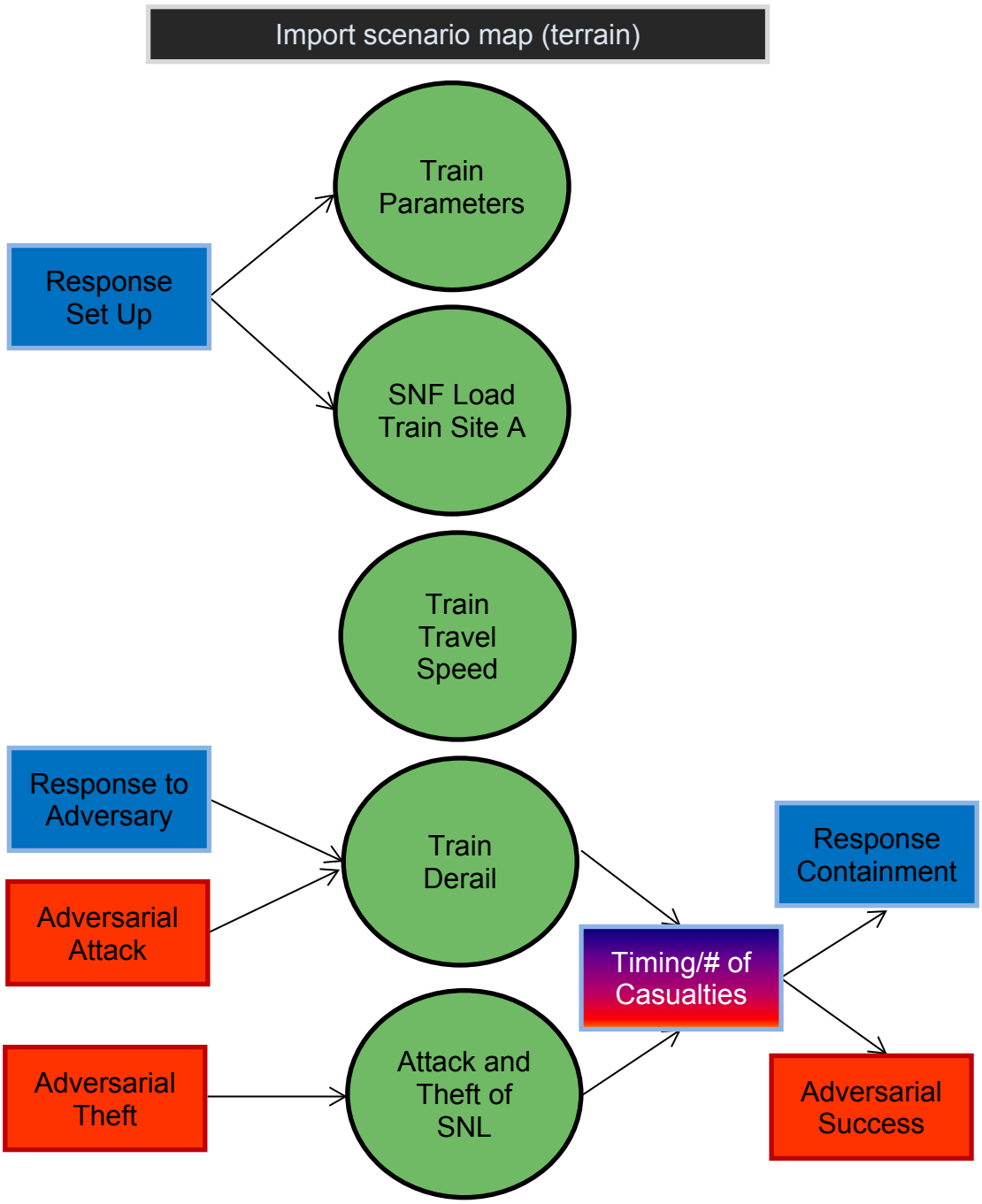

Figure 17. Scenario 1 Plan.

PRCALC Data: Scenario 1

Scenario Description

The safeguards scenario evaluated by PRCALC assumes that the accidental derailment of a shipment of SNF and a subsequent attack. The accident/attack results in the increased probability of the theft of the SNF. The scenario is modeled as a Markov model, which is a sequence of stages assigned to major model components, and probabilities of moving to a subsequent stage.

The model takes as input a variety of factors around the SNF: attractiveness to proliferators, applied safeguards measures, and intrinsic barriers put in place that would affect a diversion attempt. The model computes as outputs the detection probability at each potential stage of diversion and the probability of proliferation success or failure.

Input Parameters

PRCALC provides a user interface to enter inputs. The PRCALC input parameters include the following:

- The normal and diversion stages of the Markov model, and their connections.
- The characteristics of the reactor-grade plutonium contained in the SNF. These will depend on the reactor type (BWR or PWR), age, and burnup of the SNF shipment.
- The applied safeguards measures to the shipment of SNF.
- The intrinsic barriers of the SNF, cask, and transportation.

A detailed discussion of the above parameters is provided below.

Markov Model Stages

The stages of the Markov model for the SNF transportation Scenario 1 must be enumerated in the PRCALC user interface. Further, the interconnections between the stages must be specified. Figure 18 shows the Markov Model, and its constituent stages, for this accident/attack scenario. It has been entered into the PRCALC user interface.

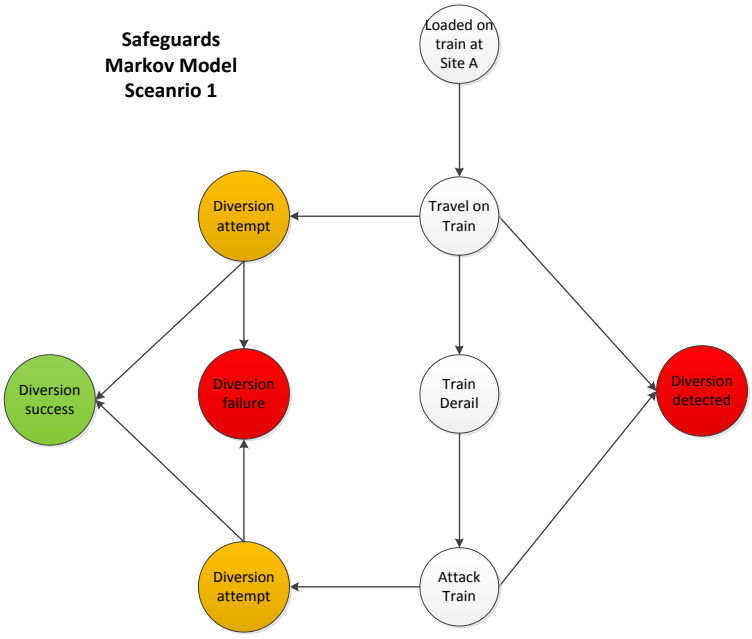

Figure 18. Markov Model for Scenario 1.

Note that the Markov model has only a couple of stages before the train accidentally derails and the shipment of SNF is subsequently attacked. From a safeguards perspective, we assume that the two major opportunities for diversion of SNF happens while the train is traveling and while it is being attacked. The train derailment is considered to be too quick and violent of an event for

any meaningful diversion to be possible. For the stages at which diversion is possible, the diversion may be detected due to applied safeguards measures, which is a terminal stage in the Markov chain. On the other hand, a diversion attempt, if not detected, may either succeed or fail based on intrinsic barriers. PRCALC will the compute probabilities of advancing to various stages based on the supplied inputs.

Characteristics of SNF

The radionuclide inventory of a spent fuel assembly is a function of fuel type (PWR or BWR), age (time from discharge), and burnup. The calculations for a typical PWR and a typical BWR assembly were done with ORIGEN. Twelve combinations of three burnups (40, 50, and 60 GWD) and four ages (5, 10, 25, and 50 years) were considered for a PWR and a BWR assembly.

The transportation cask is either a generic PWR cask with 24 assemblies or a generic BWR cask with 52 assemblies. The inventory of the PWR cask is the inventory of the PWR assembly times 24. The inventory of the BWR cask is the inventory of the BWR assembly times 52.

Note that each PWR/BWR assembly has more than 200 radionuclides. However, Pu-239 is the only one we consider from a safeguards perspective. This is because Pu-239 is considered by the IAEA to be a "direct use" material. Pu-239 is attractive to proliferators because it is fissionable and separating the plutonium from the SNF is easier than to enrich the SNF Uranium. Table 17 provides PWR and BWR Pu-239 mass for each of 12 cases. Note that 8 kg of Pu-239 is considered 1 significant quantity (SQ) according to the IAEA.

In PRCALC, several input parameters are required to fully characterize the SNF:

- The material form is SNF.
- The number of assemblies in a cask, which is dependent on the PWR/BWR cask.
- Percentage of Pu-239 mass in the assembles/cask, as referenced in Table 17.

These SNF characteristics can have distinct values for each Markov stage to allow for changing nuclear material properties in nuclear facility processes. However, for the transportation case, the characteristics of the SNF will remain the same for each stage.

Safeguards

There are many types of safeguards, or extrinsic barriers, that can be applied to the SNF to increase the probability that a diversion attempt is detected. Note the "diversion detected" state in the scenario Markov model in Section 2.1. The more safeguards that are applied, the more likely a diversion will be detected.

There are different categories of safeguards that can be applied. Some will increase the likelihood of detection, but may have drawbacks, such as increased cost or safeguards inspection time. There are four main categories of safeguards:

- Audit of various nuclear material accounting records or reports.
- Material verification, such as physical inventory verification (PIV) of all nuclear material in a nuclear energy system.
- Surveillance and monitoring.
- Containment.

PRCALC has a predefined list of safeguards that can be applied to the scenario. Some of these are more administrative in nature, and must be performed by an inspector. Others can provide containment/surveillance of the shipment of SNF, such as a seal.

The detection rate r_i determines the probability of a diversion being detected when in Markov stage *i*. The detection time T_D represents the inverse of the detection rate. Each applied safeguard *j* has an individual assigned detection time, all of which are summed to find the final detection time T_D. The formula to compute a detection time for a given safeguards measure is:

$$T_{D_{(i,j)}} = T_{I_{(i,j)}} + \frac{T_{DA_{(i,j)}} + T_{VA_{(i,j)}} C_{C_{(i,j)}}}{(1 - C_{C_{(i,j)}})}$$

In safeguards, a diversion will only be detected by a safeguards inspection. This is true even when using electronic containment and surveillance measures with real-time reporting, which could trigger a more immediate inspection, based on the safeguards agreement within a country. The average time to an inspection is represented by the value T_I. T_{DA} is the average time taken to detect an anomaly, while T_{VA} is the average time it takes to confirm and verify the anomaly was caused by diversion or misuse. Finally, C_C is a factor to model the impact of concealment activities on the part of the proliferator. In other words, this factor increases the amount of time it will take an inspector to discover a diversion.

Intrinsic Barriers

The proliferation resistance is also affected by intrinsic features of the system. Intrinsic barriers are related to detrimental properties of material (e.g., radiological release, heat generation, and toxicity) and physical design features, such as isolation barriers. Before the SNF can be diverted and transferred to the clandestine elements, the difficulties arising from intrinsic barriers must be overcome. The applied intrinsic barriers increase the amount of time it takes to divert the SNF, and can result in a diversion success or failure, as seen in the Markov model shown in Section 2.1. Taken to an extreme, an infinite number of intrinsic barriers means that diversion will fail, while no intrinsic barriers means it will succeed.

As with safeguards measures, PRCALC offers a variety of input intrinsic barriers that can be applied to a given Markov stage *i*. A new parameter, T_{DIV}, represents the diversion time for no intrinsic barriers at a given Markov stage. A diversion attempt either results in a mean time to diversion success, T_{DS}, or mean time to diversion failure, T_{DF}. A time factor *a* is proportional to the number of barriers while a time delay factor τ is the amount of time delay for a given barrier. These time parameters are computed as:

$$T_{DS_i} = (a-1)T_{DIV_i} + \tau_i \qquad T_{DF_i} = \frac{T_{DIV_i} e^{-(a-1)}}{1 - e^{-(a-1)}}$$

The calculation for T_{DIV} is based on the SNF material type attractive to proliferators, the amount of material, and the diversion rate. For our SNF scenario, we are concerned with Pu-239 and know the amount being transported in a cask from Table 17. The proliferation rate *d* for a given stage *i* and material type *j* is measured in a unitless value of sigma (1 sigma = 1.27% of material mass), which is related to the measurement uncertainty material unaccounted for (MUF) when a safeguards inspector takes a periodic inventory of material. Diverting an amount of material less than 3 sigma will take an inspector additional time to discover and verify any

anomalies/diversions. In the following equation to computer diversion time, *M* is related to the total quantity of Pu-239 in a shipment while *EQ* is related to 1 SQ of Pu-239:

$$T_{DIV} = \frac{1}{\sum_i (\frac{M_j}{EQ_j} \sum_i d_i^j)}$$

PRCALC Outputs

There are four different types of states in our Markov model. The normal state indicates the expected stages (e.g., train, road, boat) of the shipment of the SNF. The state of "Diversion Detected" indicates the detection of a diversion using the safeguards approaches. The state of "Diversion Failure" represents the failure of a diversion because the proliferator cannot overcome the intrinsic barriers. The state of "Diversion Success" can be reached only if the proliferator overcomes all safeguards, intrinsic barriers, and technical difficulties. States of "Diversion Detected" and "Diversion Failure" are absorbing states, i.e., the diversion is over once the diversion is detected, or failed due to intrinsic barriers. Note that the sum of probabilities from all branches from a given Markov state is 1.0 at any time *t*.

PRCALC computes four probabilistic outputs, where the probability is plotted against time. The time parameter is associated with how long it will take to acquire the desired amount of Pu-239, in our case 1 SQ, at the input proliferation rate. Representative plots are shown in Figure 19. They are:

- Probability of Detection (DP) measures the success in the applied safeguards and resulting inspections to detect the diversion of the SNF.
- Probability of Diversion Failure (DF) measures the success of intrinsic barriers in causing a proliferation attempt to fail.
- Probability of Technical Failure (TF) measures the technical difficulties involved in the clandestine processing of the Pu to create a weapon. For our scenario, we do not consider what happens to the SNF after it has been diverted, and this measure is not computed as part of the Markov model.
- Probability of Proliferation Success (PS) is the probability that the proliferator successfully diverted the SNF without detection.

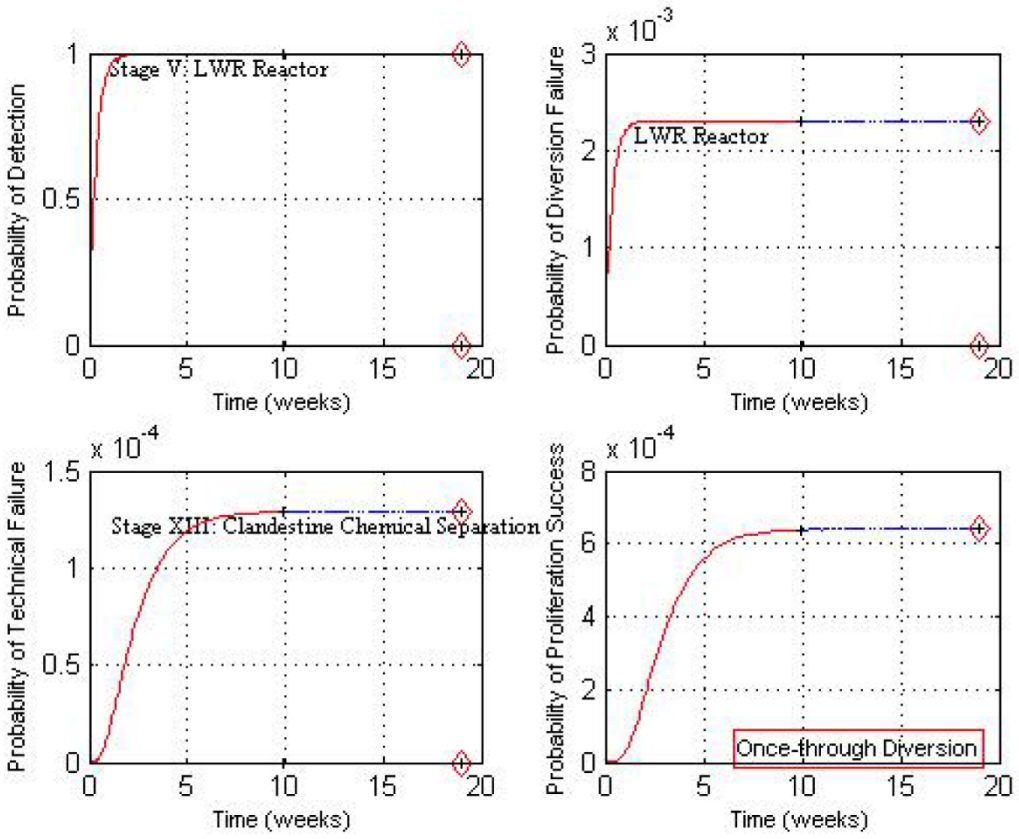

Figure 19. PRCALC Outputs.

The diversion success probability can be calculated using the other results:

$PS = 1 - DP - DF$

These probabilistic measures of proliferation resistance can be computed separately for each stage of the SNF transportation scenario, which will create a per-stage table of probabilities. Indeed, the analysis of PS at each stage can inform on where applied safeguards and intrinsic barriers could be strengthened to increase proliferation resistance. While not output by PRCALC, such other issues as proliferation cost, proliferation time, material type, and detection resource efficiency should be thought of holistically to create a picture of proliferation resistance. Some of these are inputs to PRCALC (e.g., material type of Pu) or intermediate results (e.g., proliferation time).

For this scenario, the SNF train shipment derails and is subsequently attacked. Whether the purpose of the attack is to steal the SNF or to create a radiological release, it does not make sense to calculate the DP because it will be obvious whether the SNF was stolen or breached. However, it is still possible to calculate the proliferation time after theft or think about such issues as the proliferation cost.

Table 17. PWR and BWR Pu Mass (all Isotopes) for Fuel Assemblies and Cask.

ID	60-5	60-10	60-25	60-50	50-5	50-10	50-25	50-50	40-5	40-10	40-25	40-50
Age, years	**5**	**10**	**25**	**50**	**5**	**10**	**25**	**50**	**5**	**10**	**25**	**50**
Burnup, GWD	**60**	**60**	**60**	**60**	**50**	**50**	**50**	**50**	**40**	**40**	**40**	**40**
PWR												
All Pu in assembly (kg)	3.953	3.858	3.673	3.535	3.660	3.564	3.378	3.243	3.314	3.227	3.058	2.939
% Pu-238	5.50%	5.42%	5.06%	4.31%	4.26%	4.20%	3.94%	0.033702	0.029041	0.028675	0.026877	0.022967
All Pu in 24 assemblies (kg)	94.878	92.594	88.153	84.841	87.855	85.552	81.094	77.849	79.550	77.453	73.415	70.539
All isotopes in 24 assemblies	10656.93876	10652.78	10644.3	10635.71	10744.27	10740.76	10733.5	10726.13	10832.59	10829.76	10823.8	10817.73
Total mass of one assembly (kg)	658	658	658	658	658	658	658	658	658	658	658	658
All Pu, % all isotopes	0.89%	0.87%	0.83%	0.80%	0.82%	0.80%	0.76%	0.73%	0.73%	0.72%	0.68%	0.65%
All Pu, % total assembly mass	0.60%	0.59%	0.56%	0.54%	0.56%	0.54%	0.51%	0.49%	0.50%	0.49%	0.46%	0.45%
# assemblies for 1 SQ	2.024	2.074	2.178	2.263	2.186	2.245	2.368	2.467	2.414	2.479	2.616	2.722
BWR												
All Pu in assembly (kg)	1.858	1.815	1.731	1.670	1.723	1.682	1.604	1.547	1.553	1.518	1.450	1.403
% Pu-238	3.92%	3.86%	3.59%	3.06%	2.96%	2.91%	2.71%	2.31%	1.99%	1.96%	1.82%	1.54%
All Pu in 52 assemblies (kg)	96.629	94.387	90.046	86.879	89.636	87.513	83.418	80.477	80.789	78.960	75.446	72.963
All isotopes in 52 assemblies	8419.442	8416.269	8409.717	8403.055	8488.751	8486.061	8480.439	8474.715	8557.935	8555.749	8551.127	8546.413
Total mass of 1 assembly (kg)	320	320	320	320	320	320	320	320	320	320	320	320
All Pu, % all isotopes	1.15%	1.12%	1.07%	1.03%	1.06%	1.03%	0.98%	0.95%	0.94%	0.92%	0.88%	0.85%
All Pu, % total assembly mass	0.58%	0.57%	0.54%	0.52%	0.54%	0.53%	0.50%	0.48%	0.49%	0.47%	0.45%	0.44%
# assemblies for 1 SQ	4.306	4.408	4.622	4.79	4.643	4.756	4.988	5.171	5.151	5.27	5.517	5.702

(THIS PAGE IS INTENTIONALLY BLANK)

APPENDIX C: STPA DOCUMENTATION

STPA Hierarchical Control Structures: Scenario 1

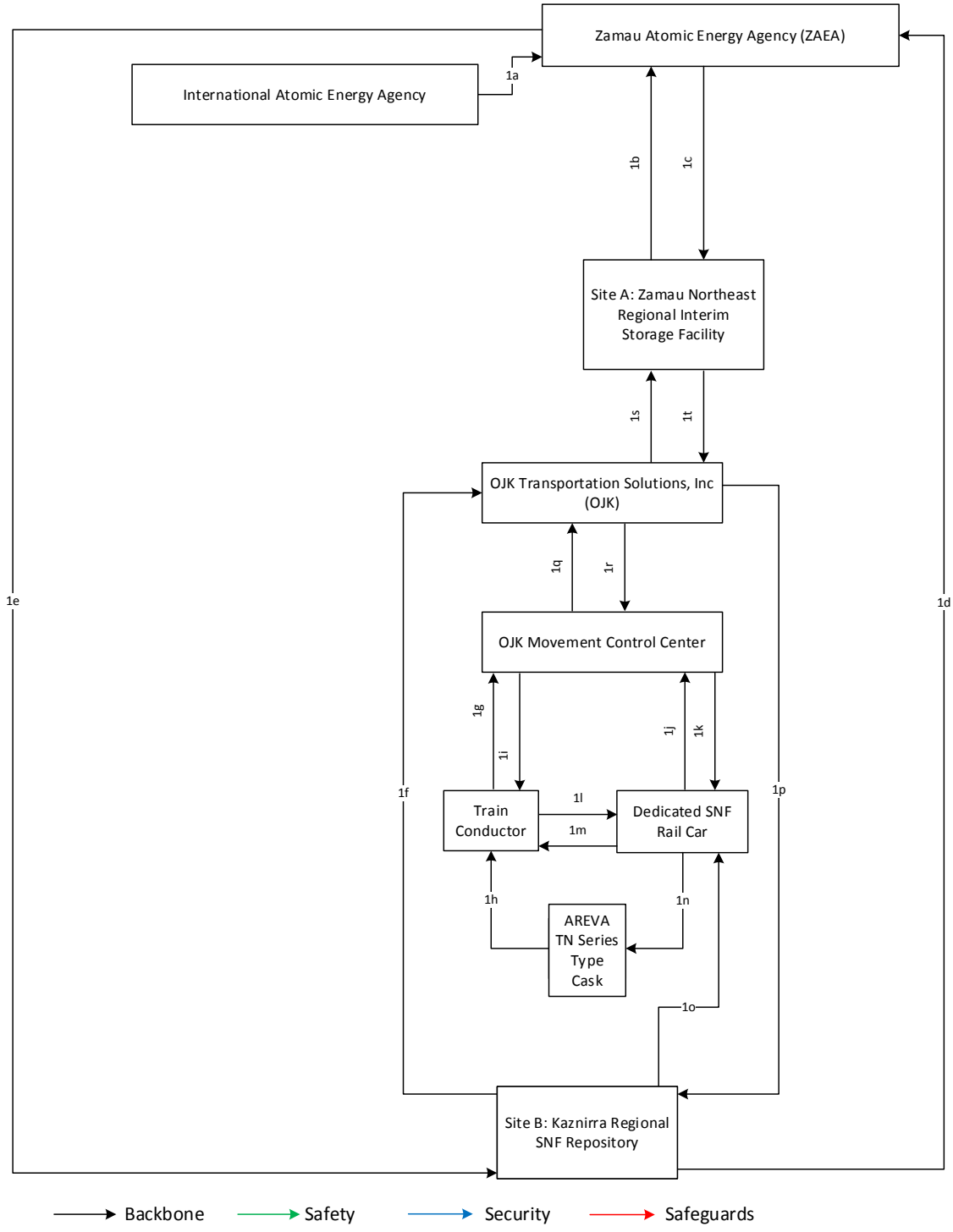

Figure 20. "Backbone" HCS for Scenario 1.

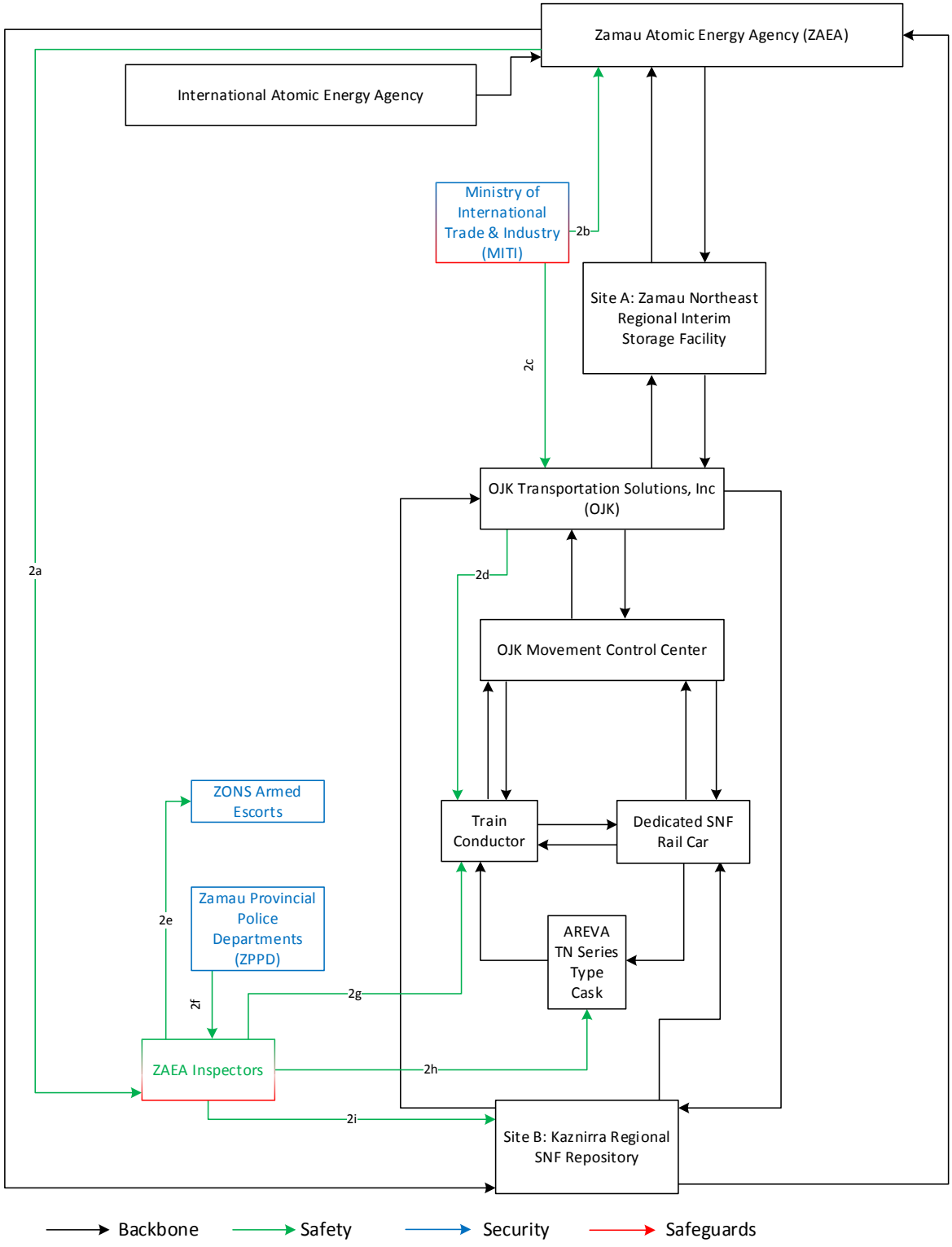

Figure 21. Safety HCS for Scenario 1.

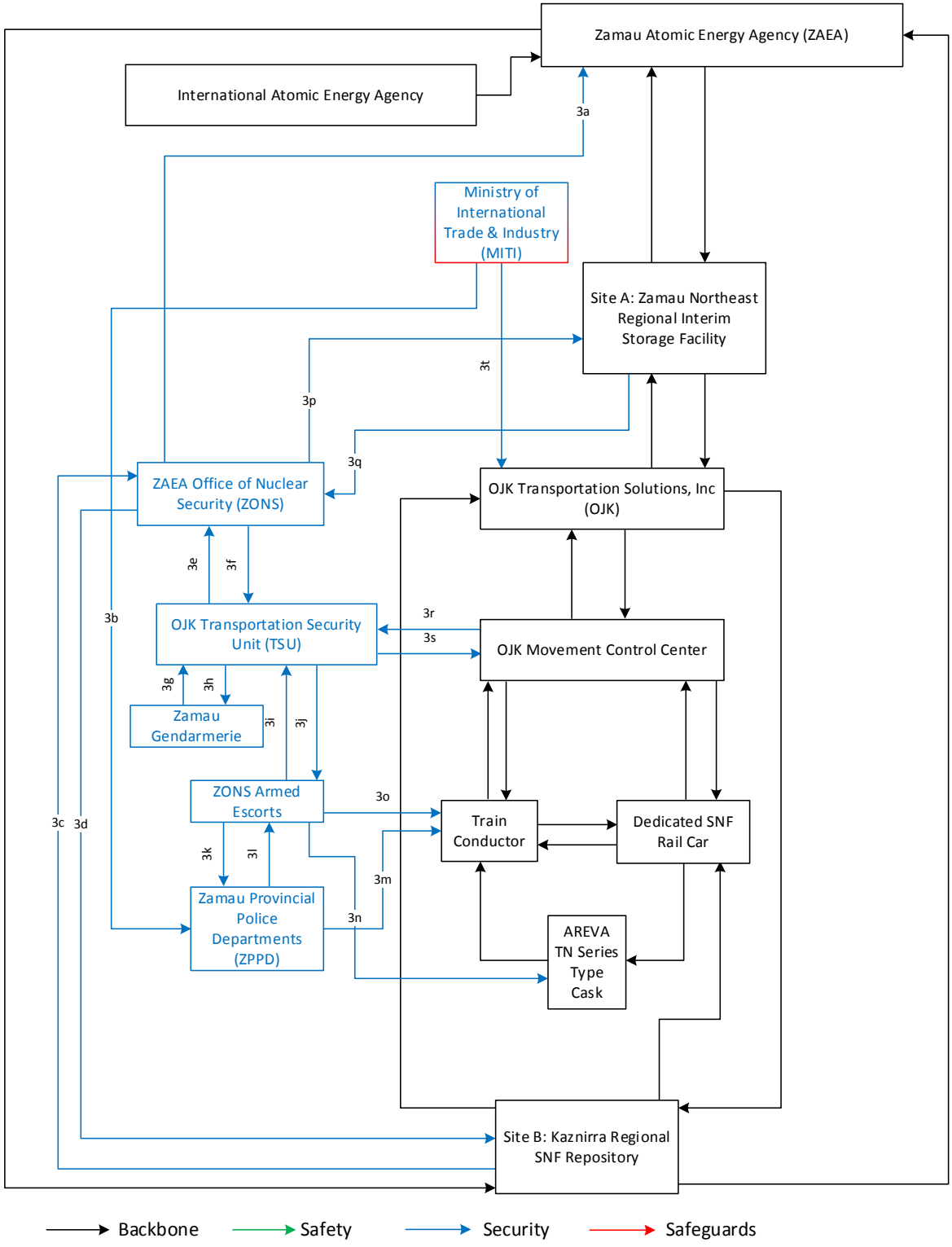

Figure 22. Security HCS for Scenario 1.

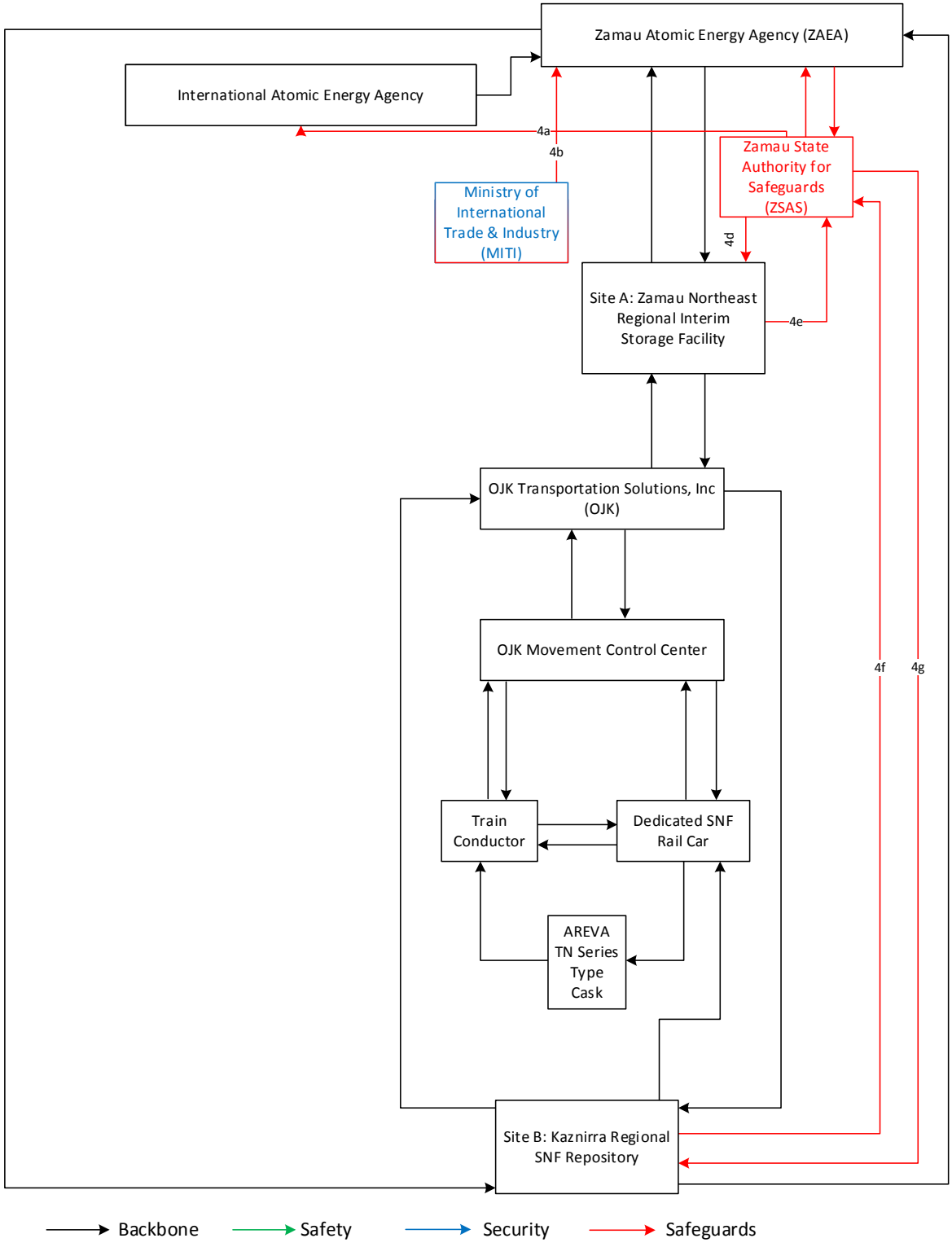

Figure 23. Safeguards HCS for Scenario 1.

STPA Controller and Control Action Table

Table 18. List of All Controllers (and Respective Control Actions) for Scenario 1.

Backbone		
Controller/Entity	**Controls**	**Feedback**
IAEA	(1a) Issues guidance on safety, safeguards, and security policy and implementation. Verifies compliance with safeguards obligations.	
National Nuclear Regulator	(1c) Reviews and approves the Facility of Departure's planned shipment schedule and process. Issues safety guidance and training guidelines.	(1b) Facility of Departure requests approval of shipment quantity and transport plans. Confirms pickup of material once transport begins.
	(1e) Reviews and approves the Facility of Arrival's planned shipment schedule and process. Issues safety guidance and training guidelines. Defines reporting requirements for confirming material arrival and makes decisions about requested exceptions to approved process.	(1d) Facility of Arrival confirms receipt of the material and associated increase in inventory.
Facility of Departure	(1b) Facility of Departure requests approval of shipment quantity and transport plans. Confirms pickup of material once transport begins.	(1c) Reviews and approves the Facility of Departure's planned shipment schedule and process. Issues safety guidance and training guidelines.
	(1t) Requests that Shipping Organization pick up material at a specified date and time.	(1s) Shipping Organization notifies Facility of Departure of current shipment status and confirms delivery of material.
Shipping Organization	(1s) Shipping Organization notifies Facility of Departure of current shipment status and confirms delivery of material.	(1t) Requests that Shipping Organization pick up material at a specified date and time.
	(1r) Shipping Organization sends required schedule and route to Movement Control Center.	(1q) Movement Control Center provides regular status updates to Shipping Organization and makes requests regarding any changes to route, schedule, or stop length.
	(1p) Shipping Organization notifies Facility of Arrival of planned delivery time and date, and provides shipment updates as needed.	(1f) Facility of Arrival confirms receipt of the material to the Shipping Organization and accepts responsibility.
Movement Control Center	(1q) Movement Control Center provides regular status updates to Shipping Organization and makes requests regarding any changes to route, schedule, or stop length.	(1r) Shipping Organization sends required schedule and route to Movement Control Center.
	(1i) Movement Control Center gives Driver instructions regarding speed, timing of breaks, and any last-minute route modifications.	(1g) Driver provides real-time updates to the Movement Control Center and notifies them of emergency situations or issues.
	(1k) Movement Control Center tracks the location of the Transportation Vehicle via GPS.	(1j) Transportation Vehicle sends location data to the Movement Control Center.

Transportation Vehicle	(1j) Transportation Vehicle sends location data to the Movement Control Center.	(1k) Movement Control Center tracks the location of the Transportation Vehicle via GPS.
	(1m) Transportation Vehicle contains the Driver and moves the Driver to the required locations.	(1l) Driver controls the speed and stopping of the Transportation Vehicle. Driver also controls and monitors vehicle fuel levels, mechanical integrity, and speed.
	(1n) Transportation Vehicle holds Cask in place via overpack or harness, provides some protection from shocks, and provides movement and momentum.	(1o) Facility of Arrival allows entry of Transportation Vehicle at the facility.
Driver	(1i) Driver provides real-time updates to the Movement Control Center and notifies them of emergency situations or issues.	(1i) Movement Control Center gives Driver instructions regarding speed, timing of breaks, and any last-minute route modifications.
	(1g) Driver provides real-time updates to the Movement Control Center and notifies them of emergency situations or issues.	(1h) Cask impacts driver's ability to control vehicle through weight/momentum.
	(1l) Driver controls the speed and stopping of the Transportation Vehicle. Driver also controls and monitors vehicle fuel levels, mechanical integrity, and speed.	(1m) Transportation Vehicle contains the Driver and moves the Driver to the required locations.
Cask	(1h) Cask impacts Driver's ability to control vehicle through weight/momentum.	(1n) Transportation Vehicle holds Cask in place via overpack or harness, provides some protection from shocks, and provides movement and momentum.
Facility of Arrival	(1d) Facility of Arrival confirms receipt of the material and associated increase in inventory.	(1e) Reviews and approves the Facility of Arrival's planned shipment schedule and process. Issues safety guidance and training guidelines. Defines reporting requirements for confirming material arrival and makes decisions about requested exceptions to approved process.
	(1o) Facility of Arrival allows entry of Transportation Vehicle at the facility.	(1p) Shipping Organization notifies Facility of Arrival of planned delivery time and date, and provides shipment updates as needed.
	(1f) Facility of Arrival confirms receipt of the material to the Shipping Organization and accepts responsibility.	

Table 18 (continued). List of All Controllers (and Respective Control Actions) for Scenario 1.

Safety		
Controller/Entity	**Controls**	**Feedback**
Escort Vehicle		(2e) Inspectors control stop time of Escort Vehicles at border crossings.
Local Law Enforcement Agency	(2f) LLE can intervene in Inspectors' work or prevent/aid their arrival via traffic controls.	
Inspectors	(2e) Inspectors control stop time of Escort Vehicles at border crossings.	(2f) LLE can intervene in Inspectors' work or prevent/aid their arrival via traffic controls.
	(2g) Inspectors tell the Driver when the shipment can proceed and can detain the Driver if there is an issue.	(2a) National Nuclear Regulator trains safety Inspectors and provides them with safety inspection instructions. NNR makes decisions on course of action if significant safety issues are identified, instructs Inspectors.
	(2h) Inspectors check Cask integrity and verify that safety seals are intact.	
	(2i) Inspectors check the material for safety at border crossing in receiving country and at Facility of Arrival and allow/disallow the facility to accept responsibility for the material based on findings.	
Ministry of Transportation	(2c) MOT relays relevant road conditions or traffic issues that may impact transport.	(2b) MOT provides NNR with list of allowable routes and provides data on road/rail conditions.
Driver		(2g) Inspectors tell the Driver when the shipment can proceed and can detain the Driver if there is an issue.
		(2d) Shipping Organization instructs the Driver on allowable speeds and trains the Driver in safety procedures.
Cask		(2h) Inspectors check Cask integrity and verify that safety seals are intact.
Shipping Organization	(2d) Shipping Organization instructs the Driver on allowable speeds and trains the Driver in safety procedures.	
Facility of Arrival		(2i) Inspectors check the material for safety at border crossing in receiving country and at Facility of Arrival and allow/disallow the Facility to accept responsibility for the material based on findings.
National Nuclear Regulator	(2a) National Nuclear Regulator trains safety Inspectors and provides them with safety inspection instructions. NNR makes decisions on course of action if significant safety issues are identified, instructs Inspectors.	(2b) MOT provides NNR with list of allowable routes and provides data on road/rail conditions.
Shipping Organization		(2c) MOT relays relevant road conditions or traffic issues that may impact transport.

Table 18 (continued). List of All Controllers (and Respective Control Actions) for Scenario 1.

Security		
Controller/Entity	**Controls**	**Feedback**
Ministry of Transportation	(3b) MOT relays information about road conditions to LLE.	
	(3t) MOT informs Shipping Organization about conditions on route that may impact security.	
Competent Security Authority	(3p) CSA instructs Facility of Departure on security procedures and could stop shipment if not adequately protected.	(3q) Facility of Departure notifies the CSA that material has left the facility.
	(3f) CSA provides training and policy guidance to Transportation Security Operations.	(3e) Transportation Security Operations notifies CSA of deviation from plans or emergencies.
	(3d) CSA instructs Facility of Arrival on security procedures and could stop shipment if not adequately protected at arrival site.	(3c) Facility of Arrival notifies CSA that the shipment has been received.
	(3a) CSA notifies NNR of any deviations from policy or changes that may affect the shipment timing or route.	
Transportation Security Operations	(3e) Transportation Security Operations notifies CSA of deviation from plans or emergencies.	(3f) CSA provides training and policy guidance to Transportation Security Operations.
	(3s) Transportation Security Operations provides security status updates and location information to the Movement Control Center.	(3r) Movement Control Center notifies Transportation Security Operations of shipment location and status and any changes to speed, break time, or route.
	(3j) Transportation Security Operations instructs Escort Vehicles and personnel on security procedures and emergency response process. TSO also informs Escort Vehicles of route and schedule.	(3i) Escort Vehicles inform Transportation Security Operations of emergencies and any deviations from transportation plan.
	(3h) Transportation Security Operations calls in "Second Wave" Response if Escort Vehicles request backup or if contact is lost with Escort Vehicles.	(3g) "Second Wave" Response provides status information to Competent Security Authority.
"Second Wave" Response	(3g) "Second Wave" Response provides status information to Competent Security Authority.	(3h) Transportation Security Operations calls in "Second Wave" Response if Escort Vehicles request backup or if contact is lost with Escort Vehicles.
Escort Vehicles	(3i) Escort Vehicles inform Transportation Security Operations of emergencies and any deviations from transportation plan.	(3j) Transportation Security Operations instructs Escort Vehicles and personnel on security procedures and emergency response process. TSO also informs Escort Vehicles of route and schedule.
	(3o) Escort Vehicles can instruct the Driver on speed or stoppage in the event of an attack, or can physically stop the Driver by obstructing the Vehicle or taking control of the Driver.	(3l) LLE could assist or interfere (getting in the way, joining or initiating attack) with the ability of the Escort Vehicles to respond to an attack.

	(3n) Escort vehicles can physically stop the Cask by obstructing the Vehicle or taking control of the Driver. They also could provide protection in an attack or cause accidental Cask damage.	
	(3k) Escort Vehicles could call for assistance from LLE or could hold LLE from reaching the cask if they interfere with operations.	
Local Law Enforcement Agency	(3l) LLE could assist or interfere (getting in the way, joining or initiating attack) with the ability of the Escort Vehicles to respond to an attack.	(3b) MOT relays information about road conditions to LLE.
	(3m) LLE controls the flow of traffic (and thereby the speed and stoppage of the Driver and Transportation Vehicle). LLE can also instruct the Driver to stop.	(3k) Escort Vehicles could call for assistance from LLE or could hold LLE from reaching the cask if they interfere with operations.
Shipping Organization		(3t) MOT informs Shipping Organization about conditions on route that may impact security.
Facility of Departure	(3q) Facility of Departure notifies the CSA that material has left the facility.	(3p) CSA instructs Facility of Departure on security procedures and could stop shipment if not adequately protected.
Facility of Arrival	(3c) Facility of Arrival notifies CSA that the shipment has been received.	(3d) CSA instructs Facility of Arrival on security procedures and could stop shipment if not adequately protected at arrival site.
National Nuclear Regulator		(3a) CSA notifies NNR of any deviations from policy or changes that may affect the shipment timing or route.
Movement Control Center	(3r) Movement Control Center notifies Transportation Security Operations of shipment location and status and any changes to speed, break time, or route.	(3s) Transportation Security Operations provides security status updates and location information to the Movement Control Center.
Driver		(3o) Escort Vehicles can instruct the Driver on speed or stoppage in the event of an attack, or can physically stop the Driver by obstructing the Vehicle or taking control of the Driver.
		(3m) LLE controls the flow of traffic (and thereby the speed and stoppage of the Driver and Transportation Vehicle). LLE also can instruct the Driver to stop.
Cask		(3n) Escort Vehicles can physically stop the Cask by obstructing the Vehicle or taking control of the Driver. They also could provide protection in an attack or cause accidental Cask damage.

Table 18 (continued). List of All Controllers (and Respective Control Actions) for Scenario 1.

Safeguards		
Controller/Entity	**Controls**	**Feedback**
Ministry of Import/Export	(4b) Ministry of I/E provides NNR with shipment paperwork collected at the border and instructs NNR on commerce border crossing requirements.	
	(4c) Provides Ministry of Transportation with "allowable" paths of transit consistent with export control laws regarding type of nuclear materials and/or origin location.	
State Authority for Safeguards	(4a) SSA reports to IAEA on Safeguards issues and requests guidance.	(4e) Facility of Departure informs State Authority for Safeguards of planned shipment and inventory reduction.
	(4d) SSA notifies Facility of Departure of Safeguards requirements and approves proposed processes.	(4f) Facility of Arrival informs State Authority for Safeguards of receipt of materials and inventory increase.
	(4g) SSA notifies Facility of Arrival of Safeguards requirements and approves proposed processes.	
National Nuclear Regulator		(4b) Ministry of I/E provides NNR with shipment paperwork collected at the border and instructs NNR on commerce border crossing requirements.
IAEA		(4a) SSA reports to IAEA on Safeguards issues and requests guidance.
Facility of Departure	(4e) Facility of Departure informs State Authority for Safeguards of planned shipment and inventory reduction.	(4d) SSA notifies Facility of Departure of Safeguards requirements and approves proposed processes.
Facility of Arrival		(4g) SSA notifies Facility of Arrival of Safeguards requirements and approves proposed processes.

STPA Step 1 Data Tables: Scenario 1

Table 19. STPA Step 1 Table for Safeguards (SGCA 1 and 2), Safety (SACA 1 and 2) and Security (SECA 1 and 2) Control Actions Evaluated Independently.

SAFEGUARDS Control Actions		Proliferation Control Actions			
#	Description	Needed, Not Provided	Provided, Not Needed	Given Too Early/Late or in Wrong Order	Stopped Too Soon/Engaged Too Long
SGCA1	Transmit GPS location of SNF cask.	• Needed, Not Provided (1) = GPS transmitter no longer with cask or no longer functioning, but safeguards location paperwork still updated and turned in. ○ Result = Cask location cannot be verified real-time except verbally. [SIR10] • Needed, Not Provided (2) = GPS transmitter no longer with cask or no longer functioning, and safeguards location paperwork not updated and turned in. ○ Result = Location of cask unknown except via verbal communication. [SIR10]	• Provided, Not Needed = N/A	**Given too early:** N/A **Given too late:** Same as not provided. **Given in Wrong Order:** Same as not provided, but with additional confusion.	**Stopped too soon:** Same as not provided. **Engaged too long:** N/A
SGCA2	Submit confirmation of removing SNF from inventory within 48 hours to IAEA.	• Needed, Not Provided (1) = Confirmation of SNF removal not provided to the IAEA. ○ Result = Untimely reporting of SNF removal, known state of SNF rods inside cask. [SIR10, SIR11]	• Provided, Not Needed (1) = Removal of SNF reported to the IAEA. ○ Result = No SIR. • Provided, Not Needed (2) = Removal of SNF reported to the IAEA, but still in place at origin site. [SIR 10]	**Given too early:** Same as Provided, Not Needed. **Given too late:** Same as Needed, Not Provided. **Given in Wrong Order:** N/A	**Stopped too soon:** Same as Needed, Not Provided. **Engaged too long:** N/A

Table 19 (continued). STPA Step 1 Table for Safeguards (SGCA 1 & 2), Safety (SACA 1 & 2) and Security (SECA 1 & 2) Control Actions Evaluated Independently.

SAFETY Control Actions		Hazardous Control Actions			
#	Description	Needed, Not Provided	Provided, Not Needed	Given Too Early/Late or in Wrong Order	Stopped Too Soon/Engaged Too Long
SACA1	Physical assessment of cask contents in appropriately sealed facility.	• Needed, Not Provided (1) = No physical assessment of cask contents, though an appropriately sealed facility exists. ○ Result = Unknown state of SNF rods inside the cask. [No SIR] • Needed, Not Provided (2) = Physical assessment of cask contents, not inside an appropriately sealed facility. ○ Result = Known state of SNF rods, but unplanned radiological releases. [SIR1, SIR2]	• Provided, Not Needed (1) = Physical assessment of cask contents in appropriately sealed facility. ○ Result = Unnecessary/unplanned radiological release to certified radiological workers. [SIR1, SIR 2] • Provided, Not Needed (2) = Physical assessment of cask contents, but not in appropriately sealed facility. ○ Result = Known state of SNF rods, but unplanned radiological releases. [SIR1, SIR2]	**Given too early:** Same as Provided, Not Needed. **Given too late:** Same as Needed, Not Provided. **Given in Wrong Order:** N/A	**Stopped too soon:** • If needed, same as Needed, Not Provided. • If not needed, same as Provided, Not Needed. **Engaged too long:** Same as Provided, Not Needed.
SACA2	Stop acceleration once at 55mph.	• Needed, Not Provided = Speed exceeds 55mph. ○ Result = Speed above allowable limit. [SIR4]	• Provided, Not Needed = N/A. Always needed once at 55mph.	**Given too early:** Speed drops below desired speed. [No SIR] **Given too late:** Speed temporarily above 55mph. [SIR4]	**Stopped too soon:** Speed exceeds 55mph. [SIR4] **Engaged too long:** Same as Given too early.

Table 19 (continued). STPA Step 1 Table for Safeguards (SGCA 1 & 2), Safety (SACA 1 & 2) and Security (SECA 1 & 2) Control Actions Evaluated Independently.

SECURITY Control Actions		Vulnerable Control Actions			
#	Description	Needed, Not Provided	Provided, Not Needed	Given Too Early/Late or in Wrong Order	Stopped Too Soon/Engaged Too Long
SECA1	Engage rail car immobilization mechanism.	• Needed, Not Provided = Railcar can be moved/rolled. ○ Result = Cask movement possible while on railcar. [SIR5, SIR6]	• Provided, Not Needed = Railcar immobilized. ○ Result = Railcar stops unexpectedly. [SIR5, SIR7]	**Given too early:** Same as Provided, Not Needed. **Given too late:** Same as Needed, Not Provided.	**Stopped too soon:** Same as Needed, Not Provided. **Engaged too long:** Same as Provided, Not Needed.
SECA2	Communicate the process for transferring armed security responsibility.	• Needed, Not Provided = Participants not informed of process. ○ Result = No awareness of process to transfer responsibility (confusion). [SIR9]	• Provided, Not Needed = Security personnel given extraneous information. ○ Result = Potential for different perceptions/expectations for security transfer. [SIR7, SIR9]	**Given too early:** Including participants forget process. [SIR7, SIR9] **Given too late:** Same as Needed, Not Provided.	**Stopped too soon:** Participants given incomplete information. [SIR7, SIR9] **Engaged too long:** Loss of attention. [SIR7, SIR9]

Table 20. STPA Step 1 Table for a 3S Control Actions Evaluation.

Control Actions		Control Action			
#	Description	Needed, Not Provided	Provided, Not Needed	Given Too Early/Late or in Wrong Order	Stopped Too Soon/Engaged Too Long
3SCA1	Transmit GPS location of SNF cask.	• Needed, Not Provided (1) = GPS transmitter no longer with cask or no longer functioning, but safeguards location paperwork still updated and turned in. ○ Result = Cask location cannot be verified real-time except verbally. [SIR10, SIR12] • Needed, Not Provided (2) = GPS transmitter no longer with cask or no longer functioning, and safeguards location paperwork not updated and turned in. ○ Result = Location of cask unknown except via verbal communication. [SIR10, SIR12]	• Provided, Not Needed = N/A	**Given too early:** N/A **Given too late:** Same as not provided. **Given in Wrong Order:** Same as not provided, but with additional confusion.	**Stopped too soon:** Same as not provided. **Engaged too long:** N/A
3SCA2	Submit confirmation of removing SNF from inventory within 48 hours to IAEA.	• Needed, Not Provided (1) = Confirmation of SNF removal not provided to the IAEA. ○ Result = Untimely reporting of SNF removal, known state of SNF rods inside cask. [SIR10, SIR11, SIR12]	• Provided, Not Needed (1) = Removal of SNF reported to the IAEA. ○ Result = No SIR. • Provided, Not Needed (2) = Removal of SNF reported to the IAEA but still in place at origin site. [SIR 10, SIR 12]	**Given too early:** Same as Provided, Not Needed. **Given too late:** Same as Needed, Not Provided. **Given in Wrong Order:** N/A	**Stopped too soon:** Same as Needed, Not Provided. **Engaged too long:** N/A

Table 20 (continued). STPA Step 1 Table for a 3S Control Actions Evaluation.

Control Actions		Control Action			
#	Description	Needed, Not Provided	Provided, Not Needed	Given Too Early/Late or in Wrong Order	Stopped Too Soon/Engaged Too Long
3SCA3	Physical assessment of cask contents in appropriately sealed facility.	• Needed, Not Provided (1) = No physical assessment of cask contents, although an appropriately sealed facility exists. ○ Result = Unknown state of SNF rods inside the cask. [SIR12] • Needed, Not Provided (2) = Physical assessment of cask contents, but not inside an appropriately sealed facility. ○ Result = Known state of SNF rods, but unplanned radiological releases. [SIR1, SIR2]	• Provided, Not Needed (1) = Physical assessment of cask contents in appropriately sealed facility. ○ Result = Unnecessary/unplanned radiological release to certified radiological workers. [SIR1, SIR2, SIR5, SIR7] • Provided, Not Needed (2) = Physical assessment of cask contents, but not in appropriately sealed facility. ○ Result = Known state of SNF rods, but unplanned radiological releases. [SIR1, SIR2, SIR 5, SIR 7]	**Given too early:** Same as Provided, Not Needed. **Given too late:** Same as Needed, Not Provided. **Given in Wrong Order:** N/A	**Stopped too soon:** • If needed, same as Needed, Not Provided. • If not needed, same as Provided, Not Needed. **Engaged too long:** Same as Provided, Not Needed.
3SCA4	Stop acceleration once at 55mph.	• Needed, Not Provided = Speed exceeds 55mph. ○ Result = Speed above allowable limit. [SIR4]	• Provided, Not Needed = N/A. Always needed once at 55mph.	**Given too early:** Speed drops below desired speed. [SIR8] **Given too late:** Speed temporarily above 55mph. [SIR4]	**Stopped too soon:** Speed exceeds 55mph. [SIR4] **Engaged too long:** Same as Given too early.

Table 20 (continued). STPA Step 1 Table for a 3S Control Actions Evaluation.

Control Actions		Control Action			
#	Description	Needed, Not Provided	Provided, Not Needed	Given Too Early/Late or in Wrong Order	Stopped Too Soon/Engaged Too Long
3SCA5	Engage rail car immobilization mechanism.	• Needed, Not Provided = Railcar can be moved/rolled. o Result = Cask movement possible while on railcar. [SIR5, SIR6]	• Provided, Not Needed = Railcar immobilized. o Result = Railcar stops unexpectedly. [SIR5, SIR7] o Result = Railcar stops near populated area. [SIR2]	**Given too early:** Same as Provided, Not Needed. **Given too late:** Same as Needed, Not Provided.	**Stopped too soon:** Same as Needed, Not Provided. **Engaged too long:** Same as Provided, Not Needed.
3SCA6	Communicate the process for transferring armed security responsibility.	• Needed, Not Provided = Participants not informed of process. o Result = No awareness of process to transfer responsibility (confusion). [SIR9] o Result = Transfer does not occur and shipment is unescorted for some period of time. [SIR5, SIR10]	• Provided, Not Needed = Security personnel given extraneous information. o Result = Potential for different perceptions/expectations for security transfer. [SIR5, SIR7, SIR9]	**Given too early:** Including participants forget process. [SIR5, SIR7, SIR9] **Given too late:** Same as Needed, Not Provided.	**Stopped too soon:** Participants given incomplete information. [SIR5, SIR7, SIR9] **Engaged too long:** Loss of attention. [SIR5, SIR7, SIR9]

DISTRIBUTION

1	MS1371	Dianna Blair, 6830
1	MS1359	Holly Dockery, 6810
1	MS0736	Richard Griffith, 8850
1	MS1371	Amir Mohagheghi, 6833
1	MS1371	Tina Hernandez, 6832
1	MS0789	Dominic Martinez, 6835
1	MS0748	Randy Gauntt, 8852
1	MS0779	Sylvia Saltzstein, 8845
1	MS0359	D. Chavez, LDRD Office, 1911
1	MS0161	Legal Technology Transfer Center, 11500
1	MS0899	Technical Library, 9536 (electronic copy)


Sandia National Laboratories