System Theoretic Frameworks for Mitigating Risk Complexity in the International Transportation of Spent Nuclear Fuel

Adam Williams[a], Douglas Osborn[a*], and Elena Kalinina[a]
[a] Sandia National Laboratories, Albuquerque, NM, USA

Abstract: In response to the expansion of nuclear fuel cycle (NFC) activities (and the associated suite of risks) around the world, this effort provides an evaluation of systems-based solutions for managing such risk complexity in multi-modal (land and water), 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 illustrates interdependency between safety, security, and safeguards (3S) risks is inherent in NFC activities that 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. This research suggests a need (and provides a way) to reprioritize United States engagement efforts to reduce global SNF transportation risks. *Note*: This paper is a summary of the final results found in Reference [1].

Keywords: Dynamic PSA, transportation, safety, security, safeguards

1. INTRODUCTION

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 mitigate 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]. Looking at a world map suggests that such cases introduce more complexity, 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), into the 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.

* dosborn@sandia.gov; Sandia National Laboratories is a multi-mission 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. SAND2018-2776-C

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 efforts to characterize integrated 3S approaches have extended preliminary studies, but remain in the conceptual space. One 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 [5]. Another example, vulnerability evaluation simulating plausible attacks (VESPA), uses traditional risk management to integrate the 3S by pairing sabotage with safety and theft with safeguards [6]. Both 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 to adequately characterize, evaluate, and manage increasing risk complexity [7]. Two system-theoretic approaches have shown promise in mitigating risk complexity: DPRA and STPA.

1.2. 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. 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 the related regional map, 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 nuclear enterprise that provides 12% of 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 strong nuclear enterprise interested in making Site B a regional SNF repository (SNF destination).

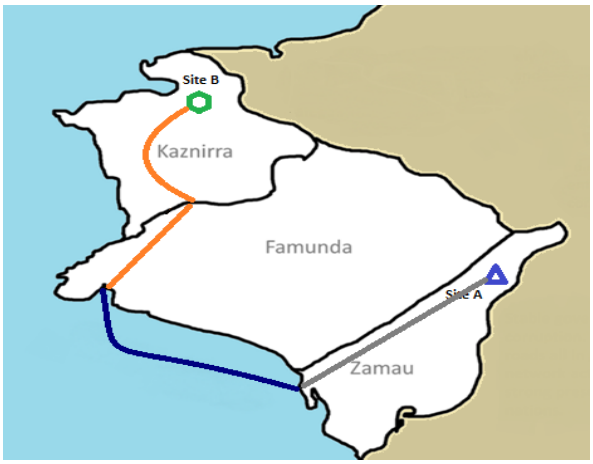

Figure 1. Regional map (and route) of hypothetical SNF transportation

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

- SNF cask loaded at origin facility (Site A) onto a rail car to the Port of Zamau (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 travels by truck to the destination facility (Site B) in Kaznirra (curved orange line).

During transit through Zamau, the train is derailed due to a 40-foot section of missing track. The derailed train[†] 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. 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. An IAEA inspector subsequently will inspect and examine the SNF shipment cask at Site A. More details can be found in Reference [8].

2. DYNAMIC PROBABILISTIC RISK ASSESSMENT

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

- A deterministic system set of models with outputs that distinguish (un)successful 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, to 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.

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. Here, the

[†] 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 [19], the first scenario for analysis included such an event.

DPRA research thrust used the Analysis of Dynamic Accident Progression Trees (ADAPT) software to generate DETs by acting as a scenario scheduler to coordinate the complex system model-related inputs and outputs between three software codes (that support traditionally isolated "S" analysis):

- *RADTRAN*[‡], 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. DPRA Branching Rules

As a DET code, ADAPT functions through a branching scheme, and 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 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 this work, branching rules were created to modify different sets of codes (summarized in Table 1). 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. 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 of a release	—	• Changes attractiveness of material • Affects physical obstacles for diversion
Degree of Notice Given to Local Law Enforcement	• Reduces public evacuation time (e.g., release)	• Shortens offsite response arrival time • (Potentially) increases adversary ability to plan, (e.g., leaks of route)	—
Discovery of Damage to Track	• Allows for train to reduce/change speed/route to avoid damaged track	—	—
Severity of Derailment	• Increases release to the environment	• Reduces the number/readiness of available response forces (e.g., injury) • Increases adversary time necessary to access cask (e.g., wreckage)	• Increases the time necessary to prepare cask for transportation
Size of Attack	—	• Affects the number of adversaries	—
State or Major Non-state Actor Sponsorship of Attack	—	• Affects levels of equipment and number of adversaries	• Sponsored attacks are a greater diversion risk

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

Branching Condition	RADTRAN Effects	STAGE Effects	PRCALC Effects
Time Necessary to Return Cask for Inspection	—	—	• Affects timeliness of safeguards reporting

2.2. DPRA Results

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. 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[§] related to safety risk for the train derailment

Group	Release Fraction		Total Release Fraction	Aerosol Fraction	Respirable Fraction	Total Respirable
	From Rods	From Cask				
Gas	0.12	Mx0.8	Mx0.096	1	1	Mx0.096
CRUD	1	0.001	0.001	1	0.05	$5*10^{-5}$
Particle	Nx $4.8*10^{-6}$	Mx0.7	NxMx $3.36*10^{-6}$	1	0.05	NxMx $1.68*10^{-7}$
Volatile	Nx $3.0*10^{-5}$	Mx0.5	NxMx $1.5*10^{-5}$	1	0.05	NxM $7.5*10^{-7}$

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 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

[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%

Lastly, PRCALC analyzed Phase 3 as an assumed successful elimination of the response forces by the adversaries, who then aim to divert a SQ 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 2) 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 [9].

[§] More specifically, for particles and volatiles (from rods to cask): N times higher than in NUREG-2125 [22] 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).

Again, the selection of this intrinsic barrier indicates how ADAPT can insert STAGE outputs as inputs into the PRCALC analysis.

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 contain different quantities of fissionable material, which influences PRCALC); and,
- Multiple types of accidents (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).

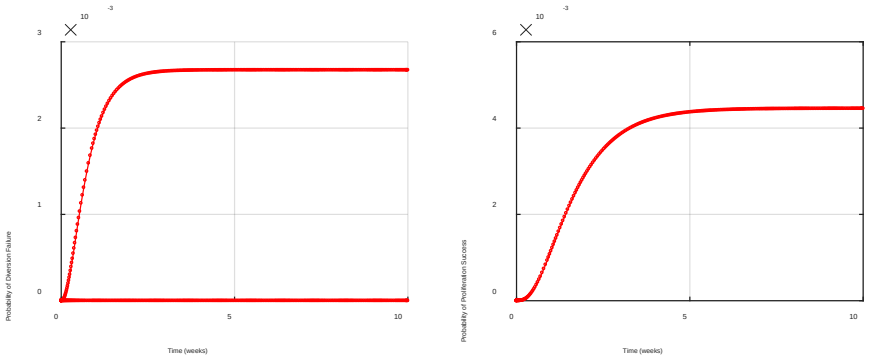

Figure 2. PRCALC generated output measures related to safeguards risk for the train derailment [9]

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

- 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.

3. SYSTEM THEORETIC PROCESS ANALYSIS

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 [10].

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: Goals or set points which higher levels within a hierarchy exhibit control of activities at lower levels based on current understanding of the system being controlled [10].
- Control structures: Hierarchical organizational structure whereby the entire socio-technical system enforces constraints to avoid undesired states through accurate and timely communication [10].
- 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) [10].

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 [10]. In general, STPA can be broken into two broad steps [10]. 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 [12]. 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" [10] support system-theoretic approaches for the design, analysis, and implementation of nuclear facilities in today's environment. 3S are recast as both emergent systems properties and control problems regarding appropriate responses of NFC activities to external disturbances or dysfunctional internal interactions. Figure 3 summarizes the STAMP/STPA process used in this research. Each step will be further explained in using scenario data.

STPA Applied to Safety: Recently, STPA has been successfully applied to hazard analysis and system safety across a broad range of socio-technical systems, including in the aviation [10], automotive [13], medical [14], and nuclear power [15] domains.

STPA Applied to Security: Similarly, recent work in critical infrastructure [16], cyber [17], port security [18], and nuclear security [12] has argued that the theoretical foundation of STAMP and STPA is highly suitable for security applications. Further, Young [17] 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, can include a wider range of underlying technical and operational influences, and is effective on real systems. In another study, Williams [18] 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.

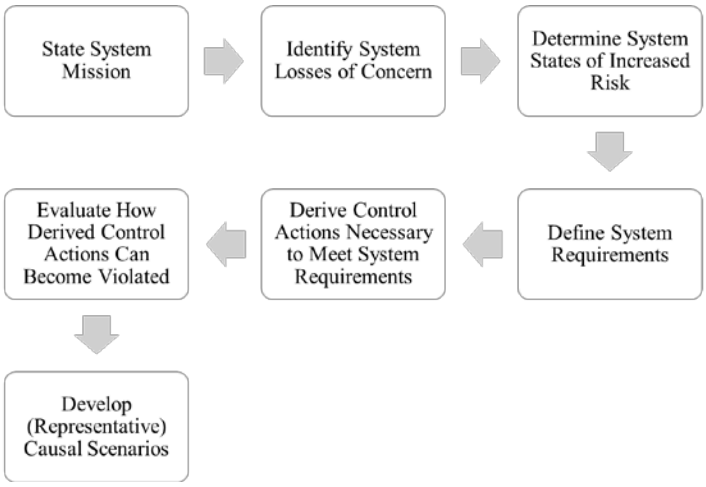

Figure 3. Summary of the logic supporting STAMP-based analysis techniques for evaluating emergent, system-level properties

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

3.1. STPA Results

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, a set of unacceptable losses for this research included serious injury or loss of life (L1), environmental contamination (L2), damage to infrastructure (L3), loss of revenue (L4), reputational/professional confidence (L5) and non-adherence to IAEA obligations (L6).

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 4). These states of increased risk are known as hazards in safety terms [10], vulnerabilities in security terms [18], and proliferation states in safeguards [9]. 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.

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.

Table 4. Representative set of states of increased risk (and their related losses) for STPA analysis of international SNF transportation.

Increased **hazardous** state [Safety]	Increased **vulnerable** state [Security]	Increased **proliferation** state [Safeguards]	**Related Losses**
Unplanned radiological release from the cask	Unauthorized access of cask	Loss of 'continuity of knowledge' of SNF material status	L1, L2, L3, L4, L5, L6
N/A	Unauthorized access of transportation vehicle	Loss of 'continuity of knowledge' of SNF location	L1, L4, L5, L6
Population/individual normal operations exposure limits exceeded	Transportation vehicle stopped longer than expected	N/A	L1, L2, L3, L4
N/A	Transportation vehicle traveling slower than scheduled	Untimely reporting of SNF arrival	L1, L2, L3, L4, L5, L6
Unconstrained movement of the cask (runaway cask)	N/A	N/A	L1, L2, L3, L4, L5
N/A	Unverified transfer of armed security responsibility	N/A	L1, L2, L3, L6
Transportation vehicle exceeds regulated speed limits	N/A	N/A	L1, L2, L4
N/A	N/A	Untimely reporting of SNF removal	L5, L6

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): The hierarchical control structure (HCS) in 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.

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. Table 5 shows the control actions evaluated for this analysis.

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 5. Summary of STPA-generated states of increased risk for a representative set of control actions for international SNF transportation.

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 too early" Subscripts denote a particular conditional description for a violated control action aligned with a given state of increased risk		

4. 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 and scenario 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 a 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 3S

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 a new system state-based concept is a helpful start for managing risk complexity in NFC activities. More specifically, by drawing on complexity and systems theories, this research addressed gaps in understanding "complex risk" as a term that encompasses (but not limited to any one) traditional definitions of risk associated with security, safety, and safeguards. For more information see References [20] or [21].

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. 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. 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 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 and STPA 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 trade-space.

ACKNOWLEDGEMENTS

The authors would like to thank the Sandia Laboratory Directed R&D committee for the opportunity to conduct such challenging, and rewarding research. We also thank the Sandia National Laboratories' Global Nuclear Assurance and Security leadership for their support through this project.

REFERENCES

[1] 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 (SAND2017-10243)," Sandia National Laboratories, Albuquerque, NM, 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] M. Stein and M. Morichi, "Safety, Security and Safeguards by Design: An Industrial Approach," *Nuclear Technologies*, no. 179, pp. 150-155, 2012.

[6] 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.

[7] 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.

[8] 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 (SAND2017-13661)," Sandia National Laboratories, Albuquerque, NM, 2017.

[9] 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.

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

[11] 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.

[12] 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.

[13] 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.

[14] 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.

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

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

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

[18] 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.

[19] 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.

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

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

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