SAND2018-2809C

Using Systems Theory to Address Complex Challenges to International Spent Nuclear Fuel Transportation

Adam D. Williams
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-1371
505-844-6779
adwilli@sandia.gov

Abstract. Simply looking at a world map suggests new, more complex set of risks and threats will challenge successful international spent nuclear fuel (SNF) transportation operations. Whether related to multimodal transfers of SNF casks or inconsistency in multijurisdictional control measures, international SNF transportation represents a clear example of new threats and risk stemming from a multifaceted, globalized operating environment. In response to recent work out of Sandia National Laboratories (SNL) suggesting that new, system-theoretic analysis techniques better ensure safe, secure and safeguarded international transportation of SNF, this paper explores the ability of basic systems theory concepts—interdependence, hierarchy and emergence—to better understand and address these complexities in system analysis.

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 an increase in the amount of spent nuclear fuel (SNF) transported across the globe. Consider the spring 1996 shipment of SNF from a research facility in Bogota to the Colombian coast for shipment back to the U.S. as part of a global program to place low enriched uranium in research reactors. A range of risks and threats facing this transportation operation included: 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 (Munera, et. al. 1997). Or, 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 challenges to successful operations (Khlpkiv & Lutkova 2010).

Simply looking at a world map suggests that these cases represent a new, more complex set of risks and threats that will challenge successful international SNF transportation operations. For example, overlaps in risk mitigation responsibilities (e.g., at ports or harbors), conflicting objectives (e.g., regulations for labeling hazardous materials in transit vs. the protective benefits of secrecy) and the increases in transfers between transportation modes (e.g., road to rail to water) and across geopolitical or maritime borders may challenge the ability to maintain safety, security, and safeguards along approved international transportation routes. Within a multifaceted, globalized environment, controls supporting successful operations may interact, as described by Olli Heinonen (former Deputy Director-General for Safeguards at the International Atomic Energy Agency [IAEA]):

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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.

> *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 (Heinonen 2017). (Emphasis added)

Traditional analysis methods struggle to describe how the dynamics of globalized environments can challenge safety (e.g., preventing an accidental radiological release), security (e.g., protecting against intentional malicious acts) and safeguards (e.g., averting state-sponsored diversion of nuclear material) control measures to mitigate and manage such risks (e.g., mitigation resources and regulations along approved international SNF transportation routes may be inconsistent). A recently completed study at Sandia National Laboratories (SNL) argued that frameworks built on basic systems theory concepts can address these challenges to better ensure safe, secure and safeguarded international transportation of SNF (Williams, et. al., 2017a).

This paper first describes the inadequacies in prior attempts to evaluate the "3S" (e.g., safety, security and safeguards and their interactions) and introduce key systems theory concepts that help frame the complexities facing international SNF transportation. Next, two recently develop analysis techniques—dynamic probabilistic risk assessment (DPRA) and system theoretic process analysis (STPA)—be described. After summarizing a hypothetical case study, the results of using these two analysis techniques (that heavily leverage these basic systems theory concepts) will be discussed. Lastly, several conclusions will be offered on the benefit of incorporating systems theory concepts into complex system analysis.

Basic Concepts in Systems Theory & New Analysis Methods

In response to simple recombinations of components not adequately describing real-world behaviors, systems theory provides a framework to evaluate the behaviors of 'many, but not infinite' components: a phenomenon sometimes called organized complexity (Bertalanffy 1972; Weinberg 1975). This perspective defines a system as a hierarchical order of processes in dynamic equilibrium (Bertalanffy 1950). Further, the laws of physics (Bertalanffy 1972) and sociology (Rasmussen 1979) suggest that ordered systems migrate toward states of greater disorder, indicating that the same end state (e.g., emergent behavior) can emerge from different initial conditions and system disturbances (Bertalanffy 1950) and different end states can emerge from the same starting conditions.

More specifically, systems theory introduces three concepts germane for addressing the safety, security and safeguards concerns for international SNF transportation: interdependence, hierarchy and emergence. Interdependence explains how interactions between components and with environmental influences can impact the ability of such components to achieve their desired objective. This concept also includes feedback, where the output of a component interactions with other components (or environmental influences) which then impacts a new set of inputs into the same component. Hierarchy refers to understanding the fundamental differences (and relationships) between levels of complexity within a system, including identifying what generates, separates and links each level. This concept also asserts that higher ranking components/influences constrain the range of possible behaviors of components/influences at lower levels. Emergence describes the phenomenon by which behaviors at a given level of complexity are irreducible to (and thus, inexplicable by) the behavior or design of its component parts. This concept helps describe how

interactions among components and environmental influences drive system-level behaviors—and, when combined with hierarchy, suggest that systems can be designed to leverage these interactions toward desired system-level behaviors.

In light of "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 [*tradeoffs between transparency of safety protocols and secrecy of security plans*]" (Leveson 2012, p. 3-4; italics added), safety, security, and safeguards are considered both emergent systems properties and control problems better addressed by incorporating basic systems theory concepts to mitigate and manage the globalized threats and risks to international SNF transportation.

Dynamic Probabilistic Risk Assessment (DPRA)

In response, dynamic probabilistic risk assessment (DPRA) uses dynamic event trees (DET) to analyze the emergent dynamics of system-level properties based on time-synched interdependencies. More specifically, this framework evaluates the evolution of event trees to describe various paths of component and environmental influence interactions between initiating events and possible end states. DPRA employs system-level models to represent complex systems and determine possible evolutions during scenarios of concern (Williams, et. al., 2017a; Rutt, et. al. 2006).

This "bottom-up" technique statistically evaluates simulation run-based data across a range of stochastically and deterministically described evolution of DETs. By employing DETs for the systematic and automated assessment of possible scenarios arising from uncertainties within complex system models, DPRA better accounts for both epistemic (e.g., arising from the model and related assumptions) and aleatory (e.g., arising from stochasticity in the system operations and environments) uncertainties to provide higher fidelity analytical conclusions for system analysis.

DPRA accounts for interdependence through the use of branching and editing rules. The former describes a time-based relationship between the actions of components (or components and environmental influences) and the latter describes the operational impact of such relationships. Here, the systems theory concepts of hierarchy and emergence help describe these time-based relationships (e.g., national regulations for initiating compensatory security measures for SNF transportation on shipping company) and operational impacts (e.g., the slowed transit pace of the SNF while compensatory security measures are implemented). Here, DPRA uses the basic systems theory concepts of interdependence, hierarchy and emergence to generate higher fidelity outputs inclusive of more complex challenges to system operations.

System Theoretic Process Analysis (STPA)

Similarly, system theoretic process analysis (STPA) is based on a recently developed causality model for complex, socio-technical systems. In this model, the System Theoretic Accident Model and Process (STAMP), a system describes 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(s). STAMP 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 at Fukushima AND the a large tsunami). As such, system losses result from flawed interactions between physical components, engineering activities, operational mission, organizational structures and social factors (Leveson 2012).

STPA is a 'top-down' process that abstracts real complex system operations into hierarchical control structures and functional control loops. Within the constraints provided by higher levels in the hierarchical control structure, STPA uses control loop logic to analyze how control actions (designed for desired system behaviors) may interact to become violated—and drive the complex system toward states of higher risk. By analyzing how needed controls are not provided (or out of sequence or

stopped too soon) and unneeded controls are provided (or engaged too long), this analysis technique identifies undesired system states across this range of potential sources of undesired system-level behaviors by exploring how requirements and desired actions interact to either mitigate or potentially increase states of risk that can lead to unacceptable losses (Leveson 2012). Further, the STAMP-derived hierarchical control structure, standard operating procedures and observations are combined to identify realistic causal scenarios for these possible violations of control actions.

STPA combines the engineered safety ideas of interdependence, hierarchy and emergence to provide additional information on which to implement technologies and create protocols to allow complex systems to operate free from unacceptable losses.

Case Study & Novel Applications

As introduced with the real-world anecdotes in the introduction, operational realities illustrate increasingly complex challenges transporting SNF successfully and without incident. Interdependence, hierarchy and emergence help to more clearly understand and appreciate threats and risks to SNF transportation in complex globalized environments. More specifically, the theoretical arguments of DPRA and STPA suggest an ability to better address such threats and risk—but through novel applications and extensions of these analysis techniques (Williams, et. al., 2017a).

International SNF Transportation Hypothetical Case Study

For demonstration purposes, a hypothetical set of countries, material characteristics, and technologies was created to account for the range of classification sensitivities associated with exploring the risks of SNF transportation.[1] This hypothetical example involves the physical transportation of SNF from an origin facility in 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 national electrical power), through the intermediary country of Famunda (a non-weapons state signatory to the NPT with rampant governmental corruption), to a destination facility in Kaznirra (a non-weapons state signatory to the NPT & Additional Protocol with a strong nuclear enterprise interested in hosting a regional SNF repository).

More specifically, this international SNF transportation route is multimodal and multi-jurisdictional. For example, the SNF cask is loaded at the origin facility onto a rail car for transportation to the Port of Zamau where it is transferred from the rail car to a barge. The SNF cask travels via international waters to the Port of Famunda where it is transferred from the barge to a heavy haul truck. The SNF cask then travels by heavy-haul truck to the Famunda/Kaznirra border crossing, handed off and ultimately to the destination facility in Kaznirra. The details within this case description and scenarios of concern (more in the next section) were briefed before a panel of subject matter experts from a range of disciplines at SNL (including spent fuel transportation/management, nuclear safety, nuclear security, and nuclear safeguards)—who indicated no glaring mistakes, omissions, or flawed logic.

Analytical Results

In addition, a scenario of concern was created to analyze this hypothetical case with DPRA and STPA. In this scenario, during transit through Zamau, the train is derailed due to a 40-foot section of missing track. The derailed train[2] 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

---

[1] 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 (Williams, et. al., 2017b)

[2] Per the relatively low track class (standards dictating railroad track quality) of Zamau's railway network and because derailments are the most common type of rail incident (Abkowitz & Bickford, 2017), the first scenario for analysis included such an event.

successful, they quickly divert the equivalent of one significant quantity (SQ) of plutonium[3] from the fuel assembly and create a radiological release by detonating explosives 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.

This scenario matches plausible threats and risks for this globalized operational environment because, for example, the cause of the derailment could be accidental (due to poor rail track quality), intentional (resulting from adversary sabotage at a known time and location to support a secondary attack on the SNF) or diversionary (to mask state-sponsored proliferation activities).

DPRA applied to the international SNF transportation case study. To capture the range of internal dynamics and environmental influences, three independent analysis techniques for evaluating safety, security and safeguards were incorporated into the DPRA analysis. Here, the safety aspects were evaluated in RADTRAN[4] (Weiner, et. al. 2013), an internationally accepted program and code for evaluating the safety risks of transporting radioactive materials; the security aspects were evaluated in STAGE (Dominguez, et. al. 2012), a Sandia-specific application of a commercial modeling and simulation program for evaluating security risks in terms of physical protection system effectiveness; and, the safeguards aspects were evaluated with PRCALC (Yue, et. al. 2008), a Markov Chain-based code (developed by Brookhaven National Laboratory) for evaluating various risks associated with safeguarding nuclear materials.

More specifically, the DPRA analysis was conducting using the Analysis of Dynamic Accident Progression Trees (ADAPT) software—a DET code that was developed jointly by SNL and the Ohio State University to coordinate with a wide variety of analysis codes. ADAPT is the overall scenario scheduler that coordinates the complex system model-related inputs and outputs between these three different software codes. DPRA and ADAPT describe the evolution of the DETs in terms of time-based phases of the scenario: Phase 1 is the train derailment itself (which is an accident scenario that previously has been studied as a standalone safety case [Kalinina, et. al. 2017]); Phase 2 involves a potential security event where adversaries attack the stopped SNF shipment (leveraging the damage and confusion caused by the accident on the security forces) in order to gain access to the SNF canister; and Phase 3 investigates the safeguards implications of a successful attack on the SNF canister (which has been previously studied as a standalone safeguards case [Thomas, et. al. 2017]). As the scenario evolves through time, ADAPT transitions between RADTRAN, STAGE, and PRCALC to evaluate how the interdependencies impact desired system-level behaviors.

The transitions between these three software codes (that describe the interdependent behaviors of safety, security and safeguards control measures) are defined in terms of the branching and edit rules summarized in Table 1. Because RADTRAN is not a dynamic software code, branching in Phase 1 could not be based on conditions that develop during the simulation, therefore ADAPT was used to perform branching similarly to a classical event tree at predefined junctions (left-hand column in Table 1) with evolution in scenario paths determined by the edit rules (second column in Table 1). Phase 2 employed the dynamic software code STAGE and allowed branching to occur at specific instances in time (associated with events in the left-hand column in Table 1) and result in multiple possible paths (based on the relationships illustrated in the third column in Table 1). Lastly, Phase 3 used the results from the STAGE analysis (itself informed by the RADTRAN analysis) to evaluate attackers that are state-sponsored with the goal of diverting spent fuel and the associated branching occurs in relation to the different states in the PRCALC Markov model (based on the relationships illustrated in the third column in Table 1) and dictated by the edit rules (the right-hand column in

[3] According to the International Atomic Energy Agency, the "approximate amount of nuclear material for which the possibility of manufacturing a nuclear explosive device cannot be excluded."

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

Table 1). As an exploratory research project, this tool-to-tool integration was performed manually—but also sowed the seeds for follow-on proposals within SNL to automate this process.

Table 1: Representative Set of Branching Conditions & Edit Rules to Link RADTRAN, STAGE, and PRCALC in ADAPT Software to support DPRA analysis of international SNF transportation.

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 change speed/ route to avoid damaged track	—	—
Severity of Derailment	•Increases release to the environment	•Reduces the number/ readiness of 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
Time Necessary to Return Cask for Inspection	—	—	• Affects timeliness of safeguards reporting

By using branching and edit rules to describe how various paths within this international SNF transportation scenario evolved, DPRA illustrated how interdependence, hierarchy and emergence can offer higher fidelity system analysis of increasing real-world complexity (Table 2). For example, rather than relying on a deterministic calculation of health effects for notional individuals assuming a radiological release (e.g., only using RADTRAN), the DPRA analysis incorporates the direct (and significant) impact that a malicious act of sabotage would have on health effects. Though seemingly obvious, this interdependence is not accounted for in traditional, individual safety analysis for SNF transportation. Similarly, hierarchy was shown to help better contextualize the analysis by linking influences between control measures. In one example, the presence of response force personnel as escorts on the SNF transportation rail car helped constrain possible violations safeguards controls—ultimately acting like an additional barrier to adversary access. Lastly, emergence helped capture the deleterious effect of a radiological release (from the derailment) on the response force.

Table 2: Comparison of DPRA analytical insights between individual & integrated analysis for international SNF transportation for representative safety, security and safeguards metrics.

Software Analysis Tool [System Behavior]	**Individual Analysis**	**Integrated Analysis (via ADAPT)**
RADTRAN [Safety]	Health effects of radiological release (capture in the *maximum exposed individual*, MEI), as a deterministic function of the cask inventory (e.g., release fraction) at the time of the (assumed) radiological release	MEI, as a deterministic function of the fuel inventory of the cask (and environmental conditions) at the time of the radiological release ***influenced*** by response force ability to prevent sabotage (e.g., $P_{(Neutralization)}$) & number of responders arriving on scene
STAGE [Security]	$P_{(Neutralization)}$, as a function of stochastic parameters of response force & adversary characteristics	$P_{(Neutralization)}$, as a function of stochastic parameters of response force & adversary characteristics ***conditioned*** on health effects of radiological release (e.g., MEI) & derailment on responders/adversaries
PRCALC [Safeguards]	$P_{(Proliferation\ Success)}$, as a function of the total amount of Pu (in terms of significant quantities) in the cask, the goal of the proliferators & effectiveness of intrinsic/extrinsic barriers	$P_{(Proliferation\ Success)}$, as a function of the total amount of Pu (in terms of significant quantities) in the cask, the goal of the proliferators & effectiveness of intrinsic/extrinsic barriers ***conditioned*** on presence of response forces as a barrier to access (e.g, $P_{(Neutralization)}$) & health effects of radiological release (e.g., MEI)

These results illustrate how DPRA (1) uses basic systems theory concepts to address system performance in complex environments; (2) demonstrates it can be extended to novel applications (e.g., coordinating three disparate analysis techniques); and, (3) offers additional insights to improve safety, security, and safeguards control measures (and their interactions) to support desired system-level behaviors.

STPA applied to the international SNF transportation case study. STPA evaluates the ability for the SNF transportation system to achieve its mission to physically move SNF from an origin facility to a destination facility without disruption (unplanned or otherwise) and to selected and approved routes, timelines, and operations. As such, the set of unacceptable losses includes human serious injury or loss of life (L1), environmental contamination (L2), significant damage to infrastructure (L3), significant loss of revenue (L4), reputational/ professional confidence (L5) and non-adherence to IAEA obligations (L6).

The underlying logic of STPA suggests that, if the system migrates into one of these states of increased risk, one additional external event could result in one of these unacceptable losses. For example, STPA argues that unauthorized access to the SNF during the transport puts the system in a state of increased risk. The specific cause or contributing factors to the unauthorized access can range from the intentional use of explosives or a cask breach from an unintentional derailment. From the STPA perspective, the goal is not to prevent these causes but to design technical, administrative and systemic controls to keep the cask from experiencing unauthorized access (e.g., entering the state of higher risk). To the extent that such controls can be designed and implemented, the SNF shipment is less likely to experience an unacceptable loss.

Table 3. summarizes a representative set of states of increased risk aligned with their safety, security, and safeguard functions for international SNF transportation. Explicitly including the interdependence between safety, security and safeguards controls helped identity additional states of increased risk that not directly aligned within one of the desired system-level behaviors—and therefore are missed by individual analysis techniques. Two examples of such '3S-based states of increased risk' include the uncoordinated implementation of operational concept(s) of operations and operational emergency plans.

Table 3: 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' (material status)	L1, L2, L3, L4, L5, L6
—	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	—	L1, L2, L3, L4
—	Transport vehicle traveling slower than scheduled	Untimely reporting of SNF arrival	L1, L2, L3, L4, L5, L6
Unconstrained movement (runaway cask)	—	—	L1, L2, L3, L4, L5
—	Unverified transfer of armed security responsibility	—	L1, L2, L3, L6
Transport vehicle exceeds regulated speed limits	—	—	L1, L2, L4
—	—	Untimely reporting of SNF removal	L5, L6

A representative set of control actions associated with each state of increased risk were evaluated rigorously and systematically in STPA to identify how they could possibly be violated; including from interactions with other control actions. Per STPA, system states of increased risk result when incorrect control actions are issued, as well as when required control actions are not issued; provided too early, too late, or out of order; or, stopped too soon or engaged too long. (NOTE: The lack of formalism, consistency, and rigor in the traditional second broad step in STPA rendered its inclusion beyond the scope of this analysis.) The traceability of possible control action violations to their associated states of increased risk (and related unacceptable losses) helps identify the benefits of evaluating the interdependence between safety, security and safeguards for systems analysis of international SNF transportation. Table 4. summarizes the states of increased risk (SIR) resulting from the loss of control for the six representative control actions previously described.

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.

Table 4: 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	State of Increased Risk (SIR) [STPA hazard type]
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]
STPA Hazard Types: 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 risk		

Comparing the states of increased risk listed in Table 4 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.

STPA also argues that violations of control actions that lead to undesired system states that are conceptually similar, a commonality across specific undesired states that is evidence for the interdependence between safety, security, and safeguards. In other words, even though a high-level security requirement can 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). Such interdependencies can be exploited to enhance operational efficiency (or, in other words, reduce costs) in complex systems operations (e.g., the assignment of basic safeguards inspection responsibilities to a safety regulatory inspector in a country with limited resources).

These results illustrate how STPA (1) incorporates basic systems theory concepts to address system performance to avoid states of increased risk in complex environments; (2) demonstrates it can be extended to novel applications (e.g., evaluating conceptually similar states of increased risk between safety, security and safeguards objectives); and, (3) increases the understanding of how to counter threats and risk from globalized environment in system analysis.

Conclusions

The results from applying both DPRA and STPA to an international SNF transportation case study demonstrate the utility for using basic systems theory concepts to better understand increasingly complex risks and threats to system operations in globalized environments. Explicitly relaxing traditional assumptions of independence between system-level behaviors (e.g., evaluating safety of international SNF transportation with only RADTRAN) provides an opportunity to leverage interactions between system components (and with environmental influences) to guide desired system-level behaviors. Designing and operating systems to leverage the ability of higher hierarchical levels to constrain behaviors of lower hierarchical levels can guide interdependent relationships toward desired behaviors (e.g., emergent system properties) and away from "unintended consequences" (e.g., interdependencies that manifest in operations in spite of assumed independence).

Using systems theory to evaluate real-world risk facing international SNF transportation, however, helped identify gaps (e.g., the potential for there to be no shipment oversight entity), interdependencies (e.g., the need to coordinate between security and emergency personnel after the notional train derailment), conflicts (e.g., inspectors may have both safety and safeguards responsibilities), and leverage points (e.g., using security procedures to maintain "continuity of knowledge") across traditional safety, security, and safeguards approaches. Further, including interdependencies (and their cumulative consequence-related effects) better aligns with real-world operational uncertainties and multi-level interactions to better describe the complexity associated with multi-model, multi-jurisdictional systems. As a result, these insights 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.

Although compelling, there are a few limitations to the insights, conclusions, and implications of this research. 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. The 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.

These insights are also useful for enhancing other ongoing complex systems research on the nuclear fuel cycle (NFC) at SNL, 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 (Forrest, et. al. 2017), providing analytical insights on a more holistic and integrated approach to how decisions manifest into actions across the socio-technical nuclear landscape (Bonin, et. al. 2017) and overcoming gaps in understanding and addressing risk complexity in NFC activities (Williams & DeMenno 2017). By incorporating these basic systems theory concepts, complex systems analysis and risk assessment offer higher fidelity results by describing challenged to NFC operations in terms of interdependencies among security, safety, and safeguards concerns and controls.

References

Abkowitz, M. & Bickford, E., 2017, "Development of Rail Accident Rates for Spent Nuclear Fuel Rail Shipments," *Proceedings of the International High Level Radioactive Waste Management Conference*, Phoenix, AZ (US).

Bonin, B.,J., et. al., 2017, '*Global Nuclear Enterprise FY17 System Study (SAND2017-TBD)*' SANDIA REPORT, Sandia National Laboratories. Albuquerque, NM (US).

Dominguez, D., et. al., 2012, 'Special Nuclear Material and Critical Infrastructure Security Modeling and Simulation of Physical Protection Systems,' *Proceedings of the IEEE International Carnahan Conference on Security Technology*. Boston, MA (US).

Forrest, R., et. al., 2017, '*A 3S Risk Assessment Approach for Nuclear Power: Safety, Security & Safeguards (SAND2017-11988)*' SANDIA REPORT, Sandia National Laboratories. Albuquerque, NM (US).

Heinonen, O., 2017, "Nuclear Terrorism: Renewed Thinking for a Changing Landscape,' Foundation for Defense of Democracies, from http://www.defenddemocracy.org/media-hit/olli-heinonen1-nuclear-terrorism-renewed-thinking-for-a-changing-landscape/.

Kalinina, E. A., et. al., 2017, 'Example of Integration of Safety and Security Using Dynamic Probabilistic Risk Assessment under A System-Theoretic Framework,' in *Proceedings of the International High Level Radioactive Waste Management Conference*. Charlotte, NC (US).

Khlopkiv, A. & A. Lutkova, 2010, '*The Bushehr NPP: Why Did It Take So Long?*,' Center for Energy and Security Studies Report, Moscow, Russia.

Leveson, N., 2012, *Engineering a Safer World: Systems Thinking Applied to Safety*, MIT Press, Cambridge, MA (US).

Munera, H. A., et. al., 1997, 'Risk associated with transportation of spent nuclear fuel under demanding security constraints: The Colombian experience,' *Risk Analysis*, 17(3), p. 381-389.

Rasmussen, J., 1979, '*On the Structure of Knowledge - A Morphology of Mental Models in a Man-Machine System Context (RISO-M-2191,'* Roskilde, Denmark: Riso National Laboratory.

Rutt, B., et. al., 2006, 'Distributed Dynamic Event Tree Generation for Reliability and Risk Assessment, *Proceedings of the International Workshop on Challenges of Large Applications in Distributed Environments*, Los Alamitos, CA (US).

Thomas, M., et. al., 2017, 'An Integrated 3S Model for Safeguards for International Transport of Spent Nuclear Fuel,' in *Proceedings of the ESARDA 39th Annual Meeting.* Dusseldorf, Germany.

von Bertalanffy, L., 1950, 'The Theory of Open Systems in Physics and Biology,' *SCIENCE*, 111, p. 23-29.

———, 1972, 'The History and Status of General Systems Theory,' *The Academy of Management Journal*, 15(4), p. 407-426.

Weinberg, G.M., 1975, *An Introduction to General Systems Thinking*, Wiley, New York, NY (US).

Weiner, R.F., et. al., 2013 '*RADTRAN 6/RadCat 6 User Guide*,' SAND REPORT, Sandia National Laboratories. Albuquerque, NM (US).

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

Williams, A.D., et. al., 2017, '*Hypothetical Case and Scenario Description for International Transportation of Spent Nuclear Fuel (SAND2017-13361)*' SANDIA REPORT, Sandia National Laboratories. Albuquerque, NM (US).

Williams, A.D., et. al., 2017, '*System Theoretic Frameworks for Mitigating Risk Complexity in the Nuclear Fuel Cycle (SAND2017-10243)*' SANDIA REPORT, Sandia National Laboratories. Albuquerque, NM (US).

Yue, M., et. al., 2008, 'A Markov Model Approach to Proliferation-Resistance Assessment of Nuclear Energy Systems,' *Nuclear Technology*, 162(1), p. 26-44.