SAND2017-10442C

Improvements in Transportation Security Analysis from a Complex Risk Mitigation Framework for the Security of International Spent Nuclear Fuel Transportation

A. D. Willliams[1]

[1] Sandia National Laboratories*, Albuquerque, NM, USA

E-mail contact of main author: adwilli@sandia.gov

Abstract. A recent study in managing the multi-modal and multi-jurisdictional risks related to the international transportation of spent nuclear fuel (SNF) describes a new framing of transportation security. This study argues that applying a complex risk mitigation framework built on the interdependence of security, safety and safeguards can improve the security design and analysis of transportation security. More specifically, the concepts of hierarchy and emergence from complexity and systems theories are combined into a state-space description of complex risk and an analytic approach that enumerates its related hypothesized causal mechanisms. This complex risk approach enables decision makers to better conceptualize and contextualize how the SNF cask, though regarded as low risk in and of itself, might exhibit higher risk behaviors that challenge security along an international transportation route.

This study also demonstrates that considering SNF transportation security as part of an integrated complex risk management framework provides higher fidelity assessments across two novel analysis techniques: dynamic probabilistic risk assessment (DPRA) and system theoretic process analysis (STPA). DPRA uses phenomenological models of system evolution and stochastic behavior to account for possible dependencies between failure events and provide a unified framework for predicting the distribution of security risk associated with international SNF transportation security. STPA uses complex, socio-technical system models (inclusive of organizational influences, environmental pressures and interdependence between components) and a top-down analytical process for linking specific design details (e.g., selection of security technologies or procedures) to support the overall system objectives of improving security (and overall complex risk mitigation) along an international SNF transportation route. The benefits of this complex risk framework were demonstrated against a set of hypothetical scenarios drawn from a wide range of publicly available reports and articles detailing SNF (specifically) and special nuclear material (SNM) transportation cases (more generally).

The results of the SNL study—which concludes that an integrated complex risk mitigation framework offers several benefits to reducing security vulnerabilities to international SNF shipments—seem expandable to improving transportation security analysis writ large. The ability of the complex risk framework to increase coordination between security, safeguards and safety (as well as mitigate conflicts that diminish security) in international SNF transportation offers lessons to all other transportation of nuclear (and radiological) materials. Being able to include contextual influences, environmental pressures and interdependencies with safety (and safeguards)—whether international or domestic—helps identify solutions more aligned with the complex realities and potential real world hazards faced by transporting nuclear and radiological materials.

Incorporating complexity and systems theories into a systems engineering framework for analyzing complex risk better addresses the non-traditional risk-related pressures and dynamics that challenge traditional

* Sandia National Laboratories is a multiprogram laboratory operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. **SAND2017-XXXX**

transportation security analysis techniques—ultimately enabling the development of improved mitigation and management strategies to ensure the protection of nuclear and radiological materials against 21st century threats.

Key Words: transportation security, spent nuclear fuel, risk, systems

1. Introduction

A recent study completed by Sandia National Laboratories (SNL) analyzed a systems-based solution for managing the complex risks of the nuclear fuel cycle (NFC) [1]. This study explored the wide array of safe, secure and safeguards risks facing the increased spread of nuclear facilities, systems and infrastructure to support increasing global demand for electricity and climate change concerns. Specifically, SNL investigated the space impeccably captured in the safety, security, and safeguards (3S) challenges of internationally transporting spent nuclear fuel (SNF).

Recent trends in new nuclear energy programs and increasingly popular 'fuel take back' agreements indicate a significant increase in the amount of SNF to be transported using multiple transportation modes (e.g., road to rail to water) and across geopolitical or maritime borders. As such, the multimodal, multi-jurisdictional nature of international SNF transportation challenges traditional risk mitigation approaches that address safety, security and safeguards individually. In the words of 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 [2]. (Emphasis added)

In response, this paper briefly reviews the major points of the SNL study—including the evaluation of an integrated 3S framework to identify gaps, interactions and conflicts missed by the traditional approaches—and discusses specific implications for reducing security risk for international SNF transportation (and other NFC activities) against 21st century threats.

2. Risk Complexity & International SNF Transportation

Drawing on complexity and systems theories, the SNL study addressed gaps in understanding risk complexity in the NFC by reconceptualizing the influence(s) of traditional and non-traditional risks (and their interactions) as 'complex risk.' For international SNF transportation, complex risk encompasses—and, therefore, is not limited to any one of—the traditional definitions of risk associated with security, safety and safeguards. Given that

different entities will have varying levels of operational responsibility for the SNF as it transits an international transportation route, the SNL study argues that complex risk accounts for the social and political contexts and dynamics that may prevent the completion of the desired safety, security and safeguards objectives. Another improvement over current traditional engineering approaches to risk is that complex risk accounts for the emergence of risk resulting from interactions among security, safety, and safeguards risks and mitigations.

2.1 A New Conceptual Approach for Risk Complexity

The SNL study showed that risk is more than the probabilistic calculations of technical component reliability (common in engineering-based approaches to risk) and must include how social dynamics influence resultant behavior(s). Rather, incorporating complexity and systems theories into engineering risk helped bridge this gap with the use of the following theoretical concepts:

- **Interdependence**, or how social and technical component interactions influence the ability of technical components to complete desired functions;
- **Emergence**, or how system level behavior results from interactions among social and technical components within in a system; and,
- **Hierarchy**, or how higher level components/influences constrain the emerging behaviors of components/influences at lower levels in a hierarchy.

Further, the SNL study used these insights to inform a novel a 'state space' description of complex risk. If all possible system states can be described by total state space (T), then there is some subset of this total state space representing all desirable system states (D) and a complementary subset representing the undesirable, or 'risky,' space (T-D) (Figure 1). Per the outcomes of the SNL study, all else being equal, being in the desirable space minimizes risk by increasing the ability of the system interactions to result in desired emergent behaviors. Complex risk is then understood conceptually as a function of the distance from the state of the system to the nearest boundary of the desired space (D). If starting in the desired state, the system goal is to counter the dynamics and pressures pushing the system toward the undesired state. If starting outside the desired state, the system goal is to move into the desired state (e.g., toward states of lower risk) as quickly as possible.

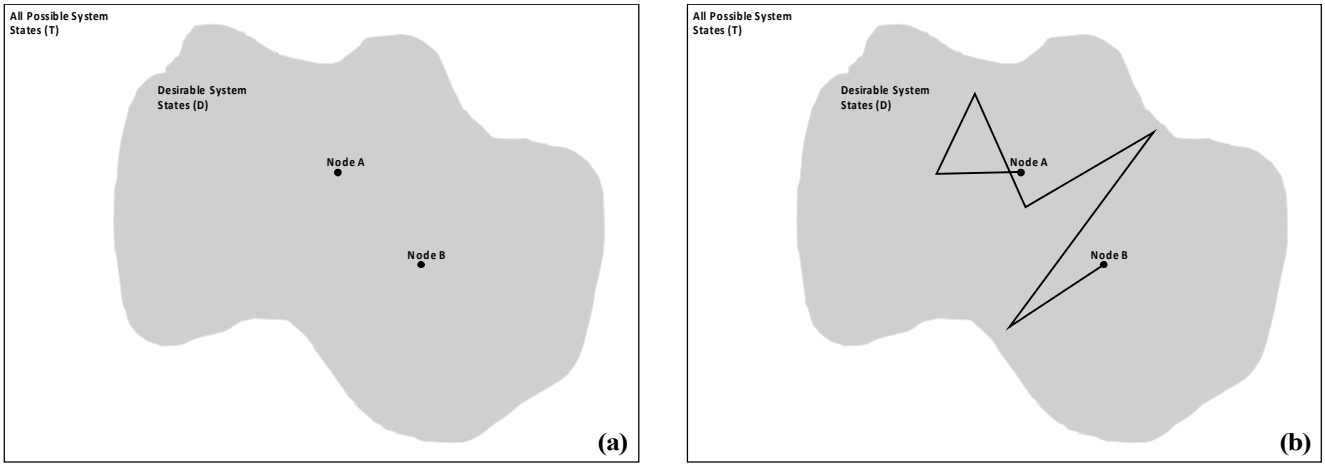

Figure 1. Static (a) and Dynamic (b) State Space Visualizations of Complex Risk, from [1].

The SNL study also argued that a system may exist at different places in the desirable space at different points in time because the requirements that define the desirable space are

implemented in different social, political, and technical contexts. The system depicted in Figure 1(a) is relatively desirable because both Node A and Node B (systems states at different points in time along an international transportation route) are centrally located within the desirable space. Yet, the SNL study concluded that complex risk is dynamic and also includes all system states between the static Nodes A and B (Figure 1(b)). While the system may appear to have relatively low risk at Nodes A and B, Figure 1(b) illustrates how there are multiples points that approach the boundary of the desirable space. (NOTE: For more details, please see [3] or [4].)

2.2 Novel Analysis Tools for Risk Complexity

Dynamic probabilistic risk assessment (DPRA) is a methodology which creates a framework to analyze the evolution of event trees that describe various paths between initiating events and possible end states. Generally, traditional probabilistic risk assessment (PRA)-based approaches focus on the rigid nature of the event logic and assume a single order of events for given scenarios—themselves commonly based on expert elicitation. There are, however, scenarios where 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 on site can substantially influence the progression of the security event. If local law enforcement arrives quickly (e.g., before any transport security escorts are killed), then the combined security response force(s) are much more likely to deter or neutralize adversary actions.

Common DPRA analysis techniques use dynamic event trees (DETs) where the system model is tracked and branches at pre-specified conditions during the scenario. The logic for creating specific branches helps determines new possible options for scenario evolution and branches, informs the associated probabilities that any one of these options will be realized and dynamically establishes the structure of the resultant event tree. The resulting DET is then 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 [5]. The SNL study demonstrated the utility of DPRA to increase the analytical fidelity of risk management for international SNF transportation.

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, systems are composed of interrelated components that maintain dynamic equilibrium through information and control feedback loops that allow it to adapt to changes in itself (or its environment) to achieve its objective [6].

Further, the System Theoretic Process Analysis (STPA) builds on the STAMP causality model and identifies undesired systems 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 general, STPA can be broken into two broad steps: (1) logically identifying potential inadequate control actions that could lead to states of increased risk (e.g., a required control action not being given or being given too late); and, (2) determining, specifically, how each potentially unsafe control action identified in the previous step could occur under operating conditions of a specific system. STPA 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 rather than ranking or prioritizing the identified states of increased risk.

Over the course of the SNL study, both DPRA and STPA demonstrated how an integrated 3S framework (based on the complex risk construct) improved safety [7], safeguards [8] and security [9] analysis for international SNF transportation.

3. Lessons from Learned from Risk Complexity in International SNF Transportation

The 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 that improve on traditional approaches (Table I).

TABLE I. Summary comparison of traditional vs. complex risk characterization of security, recreated from [9].

Attributes	Traditional Characterization (e.g., security in isolation)	Complex Risk Characterization
Risk Definition	Probabilistic ability to protect along path(s) against anticipated adversary capabilities	Emerges from potential system migration toward states of higher risk
Risk Reduction	From improved component reliability & defense-in-depth	Realized as part of complex risk management trade-space
Risk Measure	System effectiveness (e.g., combinatorial reliability of security components)	State description including nuclear material loss, area contamination & socioeconomic harms
Solution Space	Limited to increasing security component reliability or reducing adversaries capabilities	Expanded to technical, organizational or geopolitical influences & safety/safeguards leverage points
Relationship to Safety & Safeguards	None, treated as an independent risk	Parallel characteristic, treated as interdependent component of complex risk

The SNL study further concluded that the complex risk concept increased the ability to understand and manage risk in international SNF transportation—and the NFC more broadly. The study cited several key benefits of applying a complex risk approach, which included:

- distinguishing sources of risk that can be controlled (i.e., defining & implementing high level requirements) from those that cannot (i.e., external events and inherent risk associated with various modes); and,
- identifying aspects of SNF transportation routes that have considerable risk variability because of implementation with those that are relatively high-risk regardless of implementation.

This is a potential paradigm shift in risk assessment and management for NFC activities, as risk is understood from the inside out as a dynamic balance within a system state-based tradespace. The SNL study also provided major lessons learned from its system-theoretic analysis of risk complexity, which are summarized below:

- realities of international SNF transportation will challenge current approaches and assumptions;
- risk itself is complex;
- some aspects of/influences on risk are controllable, some are not;
- 3S interdependencies exist;
- risk is a complex trade space; and,
- integrated 3S risk management frameworks can reduce risk/uncertainty, even for individual (e.g., security only) perspectives

4. Implications for Transportation Security

The interdependency between nuclear safety, security and safeguards demonstrated by the SNL study indicates a need to, and provides options for, reassess how to design, implement, operate and assess security for international SNF transportation. The conclusions of the study offer a better understanding of 3S interactions that can improve SNF transportation security design and analysis. The SNL study conclusions identify a set of implications for improving transportation security (especially of SNF or along international routes) in the midst of increasing risk complexity, described in Table II, below.

TABLE II. Complex risk-based implications for SNF transportation security.

Lessons Learned from [1]	Implications for SNF Transportation Security
Realities of international SNF transportation will challenge current approaches and assumptions	• Need to (re)assess the validity of assumptions underlying current approaches to transportation security • Technical analysis tools need to account for the variation in implementation of the PPS in transit among different operators • Need to develop rigorous design for (and evaluation of) transitioning security responsibilities at geopolitical borders & conveyance changes • Need to generate a community of practitioners & best practices to create a common understanding of these challenges
Risk itself is complex	• Security risk metrics (e.g., system effectiveness, P_E) may be insufficient to adequately describe security risk/assess vulnerabilities • Need to identify key aspects/descriptors of new challenges to transportation security • Need to identify relationship(s) between technology as designed, technology as used & operational environment(s) • Need to better understand how to leverage these complexities against potential adversary action success
Some aspects of/influences on risk are controllable,	• Not all security risks lie in adversary action or can be described in probabilistic/technical reliability terms • Implementation decisions & how technical components within transportation security systems matter—and should be included in

some are not	analytical frameworks • Need to identify & evaluate 'controllable' sources of security risk (e.g., transitioning responsibilities at a geopolitical border) • Need to develop relationships between enhanced controlled over 'controllable' sources of security risk & potential adversary action success
3S interdependencies exist	• Need to change the assumption that transportation security can be accurately & adequately evaluated independently • A broader solution space exists for managing complex risk in transportation security (e.g., leveraging safeguards material accounting practices to mitigate insider issues) • Need to develop operations strategies that include identifying & managing these interdependencies • Need to identify 3S interactions between entities responsible for design, operations & evaluation in transportation security
Risk is a complex trade space	• There is no 'true' minimization of security risk, therefore attempts at security design optimization are more complex • Need to develop expertise/experience in making security-related trade-offs during international SNF transportation • Need to generate new security risk visualization tools (e.g., RIMES [10]) to capture risk complexity • Need to create a framework for understanding comprehensive effects of security design, operations & management decisions
Integrated 3S risk management frameworks can reduce risk/ uncertainty, even for individual perspectives	• Integrated approaches have been shown to incorporate more contributor to complex risk • Need to develop new analytical approaches to assess non-uniform, larger types of uncertainty (between safety, security & safeguards) • STPA & DPRA offer two novel approaches well-suited for additional evaluation for managing complex risk in transportation security • Need to create analysis tools for identifying how to leverage safety & safeguards actions for security improvement purposes

Though generated for SNF transportation, many of the same trends, influences and dynamics will be present in the international transportation of any nuclear or radiological materials.

5. Conclusion

The SNL study demonstrated how incorporating complexity and systems theories into a systems engineering framework for analyzing complex risk better addresses the non-traditional risk-related pressures and dynamics the challenge traditional transportation security analysis techniques. These insights can ultimately enable the development of improved mitigation and management strategies to ensure the protection of nuclear and radiological materials against dynamic, complex risks faced while in transit. Lastly, the insights from the SNL study offer some implications for improving SNF transportation

security—and security of nuclear materials in transit more generically—against 21st century threats.

REFERENCES

[1] WILLIAMS, A., et. al., System Theoretic Frameworks for Mitigating Risk Complexity in the Nuclear Fuel Cycle: FINAL REPORT (SAND2017-10243), Sandia National Laboratories, Albuquerque, NM (2017).

[2] HEINONEN, O., "Nuclear Terrorism: Renewed Thinking for a Changing Landscape," (2017), http://www.defenddemocracy.org/media-hit/olli-heinonen1-nuclear-terrorism-renewed- thinking -for-a-changing-landscape/.

[3] WILLIAMS, A. & M. DEMENO, "Toward a New Approach to Risk Complexity in the Nuclear Fuel Cycle," INMM Annual Meeting (Proc. of INMM 58th Annual Mttg, Palm Desert, CA, 2017).

[4] WILLIAMS, A., et. al., "A New Approach for Addressing Risk Complexity in the Nuclear Fuel Cycle," *Risk Analysis* (2017-submitted).

[5] RUTT, B., et. al., "Distributed Dynamic Event Tree Generation for Reliability and Risk Assessment", CLADE, (Proc. of Inter'l Wksp. Paris, 2006) 61-70.

[6] LEVESON, N., Engineering a safer world: Systems thinking applied to safety, MIT Press, Cambridge, Massachusetts (2012).

[7] KALININA, E., et. al., "Example of Integration of Safety and Security Using Dynamic Probabilistic Risk Assessment under A System-Theoretic Framework", IHLRWM 2017 (Proc. of ANS Inter'l Conf., Charleston, SC, 2017).

[8] THOMAS, M., et. al., "An Integrated 3S Model for Safeguards for International Transport of Spent Nuclear Fuel", ESARDA 2017 (Proc. of ESADA 39th Annual Mttg, Dusseldorf, Germany, 2017).

[9] WILLIAMS, A., et. al., "A New Look at Transportation Security: A Complex Risk Mitigation Framework for the Security of International Spent Nuclear Fuel Transportation", IAEA Conference on Nuclear Security 2016, (IAEA-CN-244, Vienna, Austria, 2016).

[10] CIPITI, B., et. al., "Security Risk Management of Small Modular Reactors," ANS PSA 2013 (Proc. of Int'l. Top. Mttg. on Prob. Safety Assess, Columbia, SC, 2013)