SAND2017-6112C

Toward a New Approach to Risk Complexity in the Nuclear Fuel Cycle

Adam D. Williams[1], Mercy B. DeMenno[1]

[1]Sandia National Laboratories*, Albuquerque, NM, USA, [adwilli; mdemenn]@sandia.gov

Abstract

The growth and evolution of safety, security and safeguards (3S) challenges to the nuclear fuel cycle (NFC)—whether stemming from asymmetries in nuclear energy program capabilities or today's dynamic environment—represent an increasing complexity in the risk associated with these activities. In real terms, 'risk' relates to those pressures and dynamics that oppose the completion of desired NFC activities. The multi-modal and multi-jurisdictional nature of international transportation of spent nuclear fuel (SNF) provides a clear example of this increasingly complex risk space. Motivated by ongoing Sandia National Laboratories (SNL) research involving an integrated 3S assessment of international SNF transportation, this paper develops a broader concept of, and technical and socio-political context, for risk. Traditional engineering approaches, such as Kaplan and Garrick (1981), define risk as a function of scenario, probability, and (adverse) consequence. While quantifying risk in this manner is often useful for comparing risk management strategies, this paper argues that quantification is not sufficient to adequately capture the real pressures and dynamics of the complex risks related to NFC activities.

In reviewing the extant engineering risk literature, a gap emerged in an area germane to the SNL project research on international SNF transportation: the inability to explain how low-risk components (e.g., SNF cask and regulated procedures) can interact non-linearly and result in higher risk, system-level behaviors (e.g., unplanned deviation from approved route). To better account for such interactions on risk resulting from transporting an SNF cask internationally (e.g., crossing geopolitical borders or changing conveyances), we introduce a new approach called "complex risk." Drawing on the concepts of interdependence, hierarchy, and emergence from complexity and systems theories, this paper formalizes a state-space description of complex risk and introduces an analytic approach that enumerates its 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 along an international transportation route. Incorporating complexity and systems theories into engineering risk better addresses non-traditional risk-related pressures and dynamics—ultimately enabling the development of improved mitigation and management strategies for NFC activities.

Introduction

The growth and evolution of safety, security and safeguards (3S) challenges to the nuclear fuel cycle (NFC)—whether stemming from asymmetries in nuclear energy program capabilities or today's dynamic environment—represent an increasing complexity in the risk associated with these activities. There are myriad safety, safeguards, and security risks associated with the set of activities comprising the nuclear fuel cycle. While some degree of risk is inevitable, these risks become significant for practitioners when they prevent the completion of desired nuclear fuel cycle activities. The multi-modal and multi-jurisdictional nature of international transportation of spent nuclear fuel (SNF) provides a clear example of the increasingly complex nature of safety, safeguards, and security risk [1]. This paper argues that approaches to the risk cycle in the engineering literature are insufficient capture the risks associated with SNF transportation. For example, the complexities involved in the international transportation of SNF have been shown to challenge traditional approaches to reducing security [2], safety [3], and safeguards [4] risk.

To address this gap, the paper develops a broader concept of risk, referred to as "complex risk." Complex risk encompasses the pressures and dynamics which prevent the completion of the desired system objectives. For example, in the case of transporting spent nuclear fuel, risk is a term that encompasses (and, therefore, is not limited to any one of the) traditional definitions of risk associated with security, safety and safeguards. Unlike many traditional engineer approaches to risk, complex risk accounts for the social, political, and technical contexts which produce these pressures and dynamics. In addition to incorporating the broader contexts for risk, complex risk accounts for the emergence of risk resulting from interactions among security, safety, and safeguards risks and mitigations. This paper applies the concept of complex risk to security for a notional SNF transportation case to demonstrate its utility on a real-world application.

Traditional Approaches to Risk

In our review of the extant engineering literature on risk summarized in Table 1[1], we identify two key challenges related to SNF transportation. First, much of the literature defines risk as a function of probability and consequence, for example: over a given set of scenarios [5]; with respect to individual utility functions [6]; in conjunction with probability of detection [7]; or as a stochastic optimization problem [8]. While probabilistic approaches to risk are a critical aspect of understanding and managing risk, we argue that by imposing the requirement of comparability among consequences implies equivalencies that conflict with psychology [9] and limit data plurality, which in turn obfuscates important sources of risk. With few exceptions (like dynamics probabilistic risk assessment [10, 11]), probabilistic approaches treat risk as static and siloed. In practice many risks are dynamic and systemic. Thus, the utility of quantifying risk as a function of probability and consequence for comparing different risks and prioritizing among risk management strategies may be limited for risks which emerge and propagate through complex socio-technical systems [9].

Second, although several scholars move beyond the consequence-oriented definition of risk to incorporate the role of both organizations and individuals [12, 13, 14], we argue that this richer accounting for micro (i.e., individual or institutional-level) behavior does not in and of itself provide sufficient legibility into macro (i.e., system-level) behavior. More specifically, many risk analysis techniques use risk mitigation at the component level to define risk mitigation at the system level. The assumed validity of this micro to macro risk extrapolation suggests that system-level behaviors are aggregations of component reliabilities and non-failing components will not result in undesired system behaviors. What results is risk analysis that relies on methods that extrapolate insights from component behavior to address system-level risk—inherently conflating component security (often measured in reliability terms) with system security [20].

Specifically, the extant literature does not offer an explanation for how low-risk components (e.g, SNF cask and its regulated procedures) can interact non-linearly to result in higher risk system-level behaviors—such as how one state's overly conservative nuclear safety policies can slow the SNF convoy road transportation speeds to levels that increase the security risk beyond designed limits. This review highlights the need for a broader conceptualization of risk to fully account for, and in turn manage, the risks resulting from transporting an SNF cask internationally. This concept of risk can inform an approach to risk analysis that is data-pluralistic, helping to avoid the limitations of purely probabilistic approaches to risk assessment. It also supports a systems theory-oriented framework aimed at avoiding the current deficits associated with the micro-macro extrapolation.

[1] This table is representative of the larger, more in-depth literature review supporting this effort. For more, please contact the authors.

Table 1. Summary of approaches to risk from multiple academic disciplines.

lName [ref] (Emphasis[2])	Summary	Advantages	Disadvantages	Analytical Gaps[3]
"Set of Triplets" [5] (Risk Definition)	• Probability *and* consequence over a given set of scenarios: Risk = $\{(s_i, p_i, x_i)\}$, i=1,2 ,..., N+1	• First level definition is computationally simple and visually accessible via risk tables or risk curves • Accounts for multi-dimensionality of consequences & incomplete information • Definition used by NRC [15]	• Requires comparability in measures of consequence • Acknowledges subjectivity in probability assessment, but does not incorporate social-psychological elements of risk	• Limited data plurality, unclear how to incorporate qualitative measures • Presumably could be applied to each "S" in isolation (assuming data could be standardized within analysis) but does not provide for interaction/feedback
Systems-Based Principles for Risk [16] (Risk Analysis, Management & Communication)	• Develops a set of 10 common principles of risk grounded in systems engineering • Defines risk as probability of an event and probability of the severity of an event	• Clearly articulates how to systems theory informs (and, possibly, unites) risk analysis • Positions these principals within a broader risk analysis approach, graphically depicted as a "roadmap"	• Application case (NextGen) is useful for demonstrating how the advocated principles are relevant but is not sufficiently analytical to provide legibility into how each principle might be operationalized	• Theoretically many of the principles are consistent with the 3S approach, although additional work is needed to translate the process as applied to NextGen to the SNF context; much of the article in on the *"what"* not the *"how"*
Knightian & Bayesian Approaches to Risk [8] (Risk Analysis)	• Defines a risk decision as "a stochastic optimization problem where the parameters and functional forms required to determine optional decisions are known"	• Resolves Knightian and Bayesian approaches to risk (objective risk, subjective risk or uncertainty, statistical risk) using complexity theory	• Although resolving theoretical differences, the implications for the practice of risk assessment are not clear, particularly outside of the field of industrial organization	• Provides useful framework for thinking about decision-making under uncertainty, but it's unclear how this framework may apply to the SNF context broadly and to integrated 3S analysis specifically
Complexity Based Risk Evaluation [17] (Risk Analysis)	• Defines complexity as "degree of difficulty in accurately predicting future behavior"	• Provides a method to move from a broad "reference definition" of complexity to specific metrics using system, observer, and behavior entropy models and presents an application case	• Requires considerable existing data/expertise about various sources of risk • Focuses mostly on the uncertainty aspect of risk (identifying causes of deviation from a system state)	• Provides a framework for disaggregating rather than aggregating risk sources and metrics • Does not address the interactions among risks
Characterizing Risk by Coupling and Tractability [18] (Risk Analysis)	• Describes risk analysis as an exercise in imagining what can go wrong (and how), this involves understanding the problem & the mechanism that gave way to the problem	• Acknowledges that different types of systems require different methods of risk analysis • Draws on Perrow's (1984) dimensions of accidents, interactive-ness and coupling, to develop a typology of various systems and risks	• Provides a very broad definition of risk: adverse outcome in some present/future state • Does not consider the potential mismatch between tools & data nor address how multiple tools might be integrated	• Safety (and presumably security by extension) is defined as the absence of the adverse outcome rather than as some desired state • Provides an approach for selection among risk analysis approaches (which we've already done) but not carrying out integrated risk assessment
Complexity Theory & the Management of Risk [19] (Risk Management)	• Risk is emergent, rather than mechanistic and as such risk managers should view organizations as ecologies, not machines	• Provides a framework for using complexity theory for risk management in complex systems • Identifies the factors that cause complex systems to "drift" into failure or success	• Does not provide a definition of risk not an actionable framework for risk analysis nor address issues related to data plurality	• Proposes a solution—diversity—which may not be feasible in the 3S context given the relative lack of centralized control and repeat players

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

Complex Risk Conceptualization

Incorporating complexity and systems theories into engineering risk better addresses risk-related pressures and dynamics not included in traditional risk analysis techniques. In operational reality, risk encompasses all of the pressures, objects and dynamics that oppose the completion of system-level goals or existence of desired system-level behavior(s). For example, Weaver (1948) describes such 'risky behaviors' in terms of two phenomena: complexity and randomness [21]. First, upon post-event analysis, there is often a logical (albeit unforeseen) pathway leading to the risky event or behavior experienced, regardless of the level of complexity within a system. The second is the level of randomness—more specifically, the accuracy of purely mechanistic or probabilistic approaches to describe the interactions within the logical pathway leading to the risky event or behavior experienced. By arguing that systems-theory is necessary to address 'risky behaviors' that are both organized and highly complex, Weaver provides a new perspective to describe "risk." Risk, then, is not just the probabilistic calculation of technical components reliably completing designed functions, but includes a description of how social dynamics influence resultant behavior(s).

Our goal is not to comprehensively define complex risk—since our contention is that complex risk is necessarily highly contextual—but rather to introduce new concept which draws on complexity and systems theories to better account for the pressures and dynamics which prevent the completion of the desired system objectives. Consistent with the Society for Risk Analysis, we identify key characteristics that describe complex risk. Specifically, we draw on the concepts of interdependence, emergence, hierarchy, and control from complexity and systems theories. First, the concept of interdependence explains how social influences can alter the ability of technical components to complete desired or necessary functions. Second, the concept of emergence explains how system level behavior can result from these interactions among social and technical system components. Third, the concept of hierarchy asserts that higher ranking components/influences constrain the emerging behaviors of components/influences at lower levels. Finally, the concept of control explains how manipulating the above phenomena to set intentional limits on lower level behaviors can cause desired behaviors emerging at the system level [22].

These insights from complexity and systems theories inform a novel approach to visualizing complex risk using a "state space" description. A state space description of risk accounts for both static and dynamic descriptions of complex risk. Beginning with the static description (Figure 1), we assume that all possible system states can be described by total state space (T). There is some subset of this total state space which represents all secure system states (S); thus, the space (T-S) is the unsecure space. The secure space is defined by high-level security requirements. We assume, all else equal, that being in the secure space minimizes risk and therefore the system objective can be understood as staying within the secure space. Therefore, complex risk can be understood conceptually as a function of the distance from the current state within the secure space to the nearest boundary and the speed at which forces are pulling/pushing the system toward the boundary of the secure space.

Because the high-level security requirements that define the secure space are implemented in different social, political, and technical contexts, a system may exist at different places in the secure space at different points in time. Figure 1 depicts the position of a system within the secure space at two different time intervals, Node A and Node B. Given the definition above, we might assume that the system depicted in Figure 1(a) is relatively secure because both Node A and Node B are centrally located within the secure space (i.e., they are relatively far away from the system boundary).

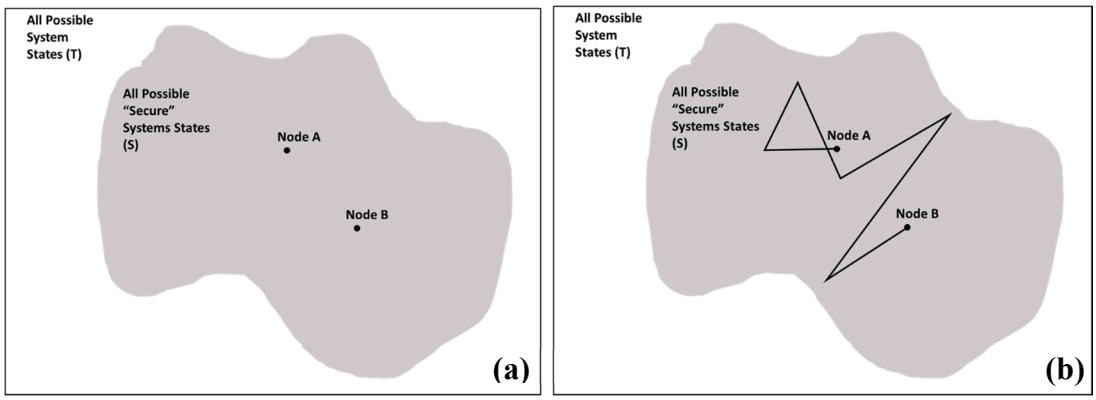

Figure 1: (a) Static state space & (b) dynamic state space description of complex risk.

However, complex risk is dynamic and therefore the risk profile for a given system involves not only a point estimate of risk for two time intervals, but also all system states between the two points, as depicted in Figure 1(b). While the system may appear relatively secure at Nodes A and B, Figure 1(b) depicts how there are multiples points that approach the boundary of the secure space.

Complex Risk & Spent Nuclear Fuel Transportation

To demonstrate the utility of the proposed complex risk concept to the nuclear fuel cycle, we provide a case example related to the international transportation of SNF. Specifically, this example involves the physical transportation of SNF from an origin facility in Zamau, through the intermediary country of Famunda, to a destination facility in Kaznirra. A regional map of our hypothetical SNF transport case study is shown in Figure 2, below (NOTE: A more complete description of this case study is provided in [23]), and includes the following fictitious nations:

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

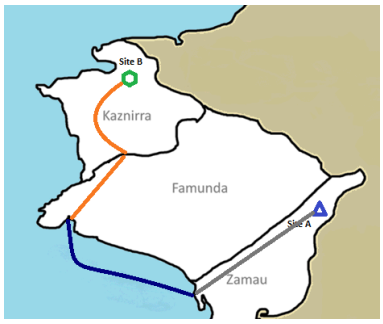

Figure 2. Regional map (and route) of hypothetical SNF transportation.

For simplicity, this explanation of "complex risk" will focus on the "organized complexity" of providing security for the SNF transportation along the first leg of the international route. Per Figure 1, this portion of the transportation route includes:

- SNF cask loaded at the origin facility onto a rail car for transportation to the Port of Zamau;
- SNF cask transferred from rail car to barge at Port of Zamau;
- SNF cask travels via international waters to the Port of Famunda;
- SNF is transfer from barge to truck at Port of Famunda; and,
- SNF cask travels by truck to the Famunda/Kaznirra border crossing.

Regional geopolitical instability (including governmental corruption), the existence of some strong insurgent groups and highly inconsistent transportation infrastructure dictates this multi-model, multi-country transportation route. As such, there are various levels of resources provided for SNF security despite that each of these countries are parties to the Convention on the Physical Protection of Nuclear Material (CPPNM) and have also all signed the CONA Treaty establishing a regional nuclear weapon-free-zone. Further (and consistent with international best practice), each country in this region agrees that the country in which the SNF transportation vehicle is currently in will provide additional security and emergency response, as necessary. It is also agreed Zamau maintains responsibility throughout barge transport since that leg may (partially) occur in international water. In addition, all employees with a security responsibility for securing SNF while its transited inside Zamau undergo a vigorous background investigation prior to being hired. To date, there have been no disputes over labor issues and no attempts to breach local nuclear facilities or transports. In Famunda, there is no background investigation provided to any personnel associated with security responsibility for securing nuclear materials and there is a growing number of low-level disputes over labor issues by contract-based security forces.

Per Figure 1, the system goal is to stay within the secure space (S)—where for this case the secure space is (partially) defined by the tenets in the Convention on the Physical Protection of Nuclear Material (CPPNM). More specifically, the operational goal is the physical transportation of SNF from an origin facility in Zamau to the Famunda/Kaznirra border crossing without disruption—unplanned or otherwise—to selected and approved routes, timelines, and operations. This goal encompasses two individually necessary but insufficient, and jointly sufficient, conditions for meeting the desired system objective. First, it requires the transportation of SNF material from the origin facility to the border crossing (i.e., the "task" depicted in the columns in Figure 3). Second, it requires meeting the operational conditions, which in this are defined as utilizing the selected and approved routes, timelines, and operations (i.e., the "condition" depicted in rows in Figure 3).

As Figure 3 depicts, this conceptualization enables a richer understanding of pressures and dynamics which lead to an outcome other than completing the desired system objective [C]. For example, the SNF materials might be successfully moved from origin to destination, but—for example, due to deviations in approved route—do so in a way that is significantly riskier than anticipated [A]. Similarly, the convoy might adhere to selected and approved routes, timelines, and operations but for reasons outside these operational conditions—such as failure in communication, for example, because of inaccurate translation or transliteration—SNF materials are not moved from origin to the border crossing [D]. Thus, complex risk encompasses pressures and dynamics which prevent the completion of the desired system objective [C].

For this scenario, all possible system states can be described by total state space (T). The secure space (S) represents all secure system states, while unsecure system states (T-S) represent all system states that are not secure. Here, the secure space defined by security design requirements which are established in the CPPNM (e.g., appropriate levels of response forces) and therefore are agnostic to the implementation contexts. Thus, with the same system requirements, risk will vary depending on context (as depicted in Figure 4 by position within the secure space). Staying within the secure space (S) is the system objective while the operational objective (C) is the physical transportation of SNF from an origin facility in Zamau to the Famunda/Kaznirra border crossing without disruption—unplanned or otherwise—to selected and approved routes, timelines, and operations.

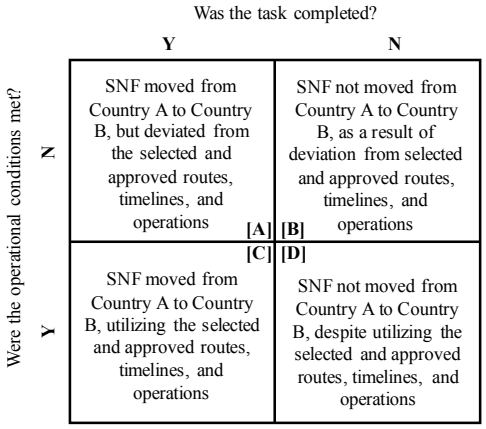

Figure 3. Logic relating system objective to "complex risk" & its state-space description.

We assume that for a given system, there is an unknown probability of some security incident (Z), which can prevent the completion of (C). In this example, Z is an attempt by an adversary (or other unauthorized individual) to access the cask while in transit. While it may be impossible to mitigate the likelihood of Z, we can manage the consequence of Z (i.e., the probability of C given Z). As described above, complex risk encompasses pressures and dynamics which prevent the completion of the desired objective. Here, the system objective (staying in the safe space) is related to the operational objective (the physical transportation of SNF without disruption to selected and approved routes, timelines, and operations) because meeting the system objective increases the probability of meeting the operational objective (C), assuming some incident (Z).

As described above, the route consists of the origin facility in Zamau, the Famunda/Kaznirra border crossing, and five transportation legs ($L_{1\text{-}5}$). While some simplifying assumptions are necessary to divide the route into legs by transportation mode, doing so enables conceptualization of discrete intervals for which an individual risk score can be assigned. We assume that the origin and destination have relatively similar levels of riskiness. Table 2 summarizes three scenarios with the same system and operational goals, origins and destinations, and routes, but different relative risks.

While the relative riskiness of the origin and the destination are constant, risk varies throughout the route and across the scenarios for two reasons. First, each transportation mode has an inherent level of risk which is outside the control of operators. For example, from a security perspective, movement on a truck is the riskiest, followed by movement on a train, and then movement on a barge; with this risk level based on the ability of an adversary to access the cask while in transit via different modes. Transfer points are the most vulnerable because the transfer of authority between stakeholders may result in gaps [2]. Second, countries have autonomy in deciding how the implement the high-level security requirements that compose the secure space. Implementation choices will vary both within countries and across countries.

In this example, Zamau has three approaches to meet the high-level security requirement for an armed escort: Special forces (high security), contract security forces (medium security), or local law enforcement (low security), each of which is sufficient to meet the high-level requirement but which varies in the operational level of security. In contrast, Famunda has two approaches to meet the high-level security requirement for an armed escort: contract security forces (medium security) or local law enforcement (low security). Unlike Zamau, Famunda might also choose to not meet the high level security requirement thereby violating the tenets of the CPPNM. Table 2 below depicts the

country implementation approaches across three hypothetical scenarios: orange, blue, and purple. Figure 4 provides a conceptual (as opposed to geographic) map of the risk described in Table 2. As described, the different risk profiles for each scenario are driven by both the inherent risk of each leg and the choices made in implementing the security requirements.

Table 2. SNF transportation scenarios[4] for "complex risk" comparison within a hypothetical spent nuclear fuel transportation case.

SNF Transportation Route Legs	**Country**	**Implementation Approach to Meet High-Level Security Requirement: Armed Escort**		
		Orange Scenario	**Blue Scenario**	**Purple Scenario**
Origin	Zamau	n/a	n/a	n/a
Movement on rail line (L_1)	Zamau	Special forces	Contract security forces	Local law enforcement
Transfer rail to barge (L_2)	Zamau	Special forces	Contract security forces	Local law enforcement
Movement on barge (L_3)	Zamau	Special forces	Contract security forces	Local law enforcement
Transfer barge to truck (L_4)	Famunda	Contract security forces	Local law enforcement	Nothing
Travel on truck (L_5)	Famunda	Contract security forces	Local law enforcement	Nothing
Arrival at border crossing with Kaznirra	Famunda/ Kaznirra	n/a	n/a	n/a

In the orange scenario, both Zamau and Famunda meet the high-level security requirement and do so with the respectively most secure implementation strategies available: Zamau provides special forces for movement on rail and barge and Famunda provides contract security focuses for movement on truck. While there is some inherent risk associated with the transfer points, particularly transfer from the barge to the truck (L_4), the orange scenario is quite secure throughout the route as depicted by its relative centrality in the secure state (S) in Figure 4. Because the system objective of staying in the secure space is met, this complex risk approach argues a relatively high probability of meeting the operational objective (C), given a potentially disruptive security incident (Z).

In the blue scenario, both Zamau and Famunda meet the high-level security requirement with the respectively moderately secure implementation strategies: Zamau provides contract security forces for movement on rail and barge and Famunda provides local law enforcement for movement on truck. Note that while Famunda's most secure implementation strategy is equivalent to Zamau's moderately secure implementation strategy (i.e., contract security forces), the modes over which Zamau has authority are inherently lower risk than those over which Famunda has authority. Because the system objective of staying in the secure space is met but there are several legs for which the system approaches the secure space boundary—including transfer from barge to truck (L_4) and movement on truck (L_5)— this complex risk approach argues a moderate probability of meeting the operational objective (C), given a potentially disruptive security incident (Z)

In the purple scenario, Zamau meets the high-level security requirement, but does so with the least secure implementation strategy available: local law enforcement. Famunda fails to meet the high-level security requirement, meaning that the cask is traveling by truck (itself the riskiest mode), without an armed escort, for one leg (L_5). The relatively high risk of the purple scenario is depicted by the spread of its risk map in Figure 4 and its movement outside the secure space for the both the transfer from barge to truck (L_4) and movement on truck (L_5). As a result, this complex risk approach

[4] We made several simplifying assumptions in this table, including: that there is a single high-level security requirement—armed escort—which defines the secure space and that all legs, including transfer points, are confined to a single country.

argues a relatively low probability of meeting the operational objective (C), given a potentially disruptive security incident (Z).

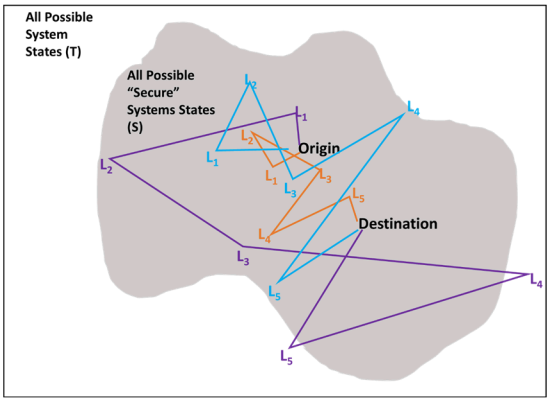

Figure 4. Illustration of the "complex risk" state space description for three scenarios within a hypothetical spent nuclear fuel transportation case.

Summary & Conclusions

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

The application of the complex risk concept to the SNF transportation case yields several insights which both speak to the utility of the complex risk concept and state space description for this case—and for understanding and managing risk in the NFC more broadly. First, this application case distinguishes the sources of risk than can be controlled (i.e., defining high level security requirements, implementing high-level security requirements) from those that cannot (i.e., security incident (Z), inherent risk associated with various modes). Second, this application case enables the identification of aspects of the route that have considerable risk variability because of implementation with those that are relatively high-risk regardless of implementation (e.g., L_4 in Figure 4). Finally, this application case highlights the need for greater attention to scenarios in which the system objective is not completed, but for reasons other than violating the conditions (i.e., Scenario D in Figure 3). This potential outcome suggests the possibility that the source of failure is not anticipated by high-level security requirements which comprise the secure space (S), suggesting a possible need to revisit these requirements. Furthermore, it underscores the value of understanding risk as not only a probabilistic calculation of technical components reliably functioning, but also a result of the interaction of technical components and social dynamics.

Further research is needed to more fully explore the theoretical limits and operational applicability of this "complex risk" concept. In response, our current research is expanding this application case to an integrated security, safety and safeguards ("3S") analysis of this international SNF transportation case and the development of a more developed socio-technical system framework for complex risk. Ultimately, our "complex risk" concept is aimed to support new frameworks and analytical techniques to more efficiently and effectively capture (and mitigate) the increasing complexity facing the nuclear fuel cycle in rapidly changing, dynamic implementation environments.

References

[1] E. Kalinina and I. K. Busch, "Transportation of Spent Nuclear Fuel from Reactor Sites in the US—What Will It Take?," in *International High-Level Radioactive Waste Management Meeting*, Charlotte, NC, 2015.

[2] A. D. Williams, D. M. Osborn, K. A. Jones, E. A. Kalinina, B. Cohn, M. J. Parks, E. R. Parks, E. Johnson and A. H. Mohagheghi, "A New Look at Transportation Security: A Complex Risk Mitigation Framework for the Security of International Spent Nuclear Fuel Transportation," in *IAEA International Conference on Nuclear Security (CN-244)*, Vienna, Austria, 2016.

[3] E. Kalinina, B. Cohn, D. Osborn, J. Cardoni, A. D. Williams, M. J. Parks, K. Jones, N. Andrews, E. Johnson, E. Parks and A. Mohagheghi, "Example Of Integration Of Safety, Security, And Safeguard Using Dynamic Probabilistic Risk Assessment Under A System-Theoretic Framework," in *International High-Level Radioactive Waste Management Meeting*, Charleston, SC, 2017.

[4] M. Thomas, A. Williams, K. Jones, D. Osborn, E. Kalinina, B. Cohn, M. J. Parks and A. Mohagheghi, "An Integrated 3S Model for Safeguards for International Transport of Spent Nuclear Fuel," in *European Safeguards Research and Development Association Annual Meeting 2017*, Dusseldorf, Germany, 2017.

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

[6] A. Pollatsek and A. Tversky, "A Theory of Risk," *Journal of Mathematical Psychology,* vol. 7, pp. 540-553, 1970.

[7] S. E. Griffis and J. M. Whipple, "A Comprehensive Risk Assessment and Evaluation Model: Proposaing a Risk Priority Continuum," *Transportation Journal,* pp. 428-451, 2012.

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

[9] G. Wyss, "The Accident That Could Never Happen: Deluded by a Design Basis," in *Learning from a Disaster: Improving Nuclear Safety and Security after Fukushima*, Stanford, Stanford University Press, 2016, pp. 29-57.

[10] A. Hakobyan, T. Aldemir, R. Denninga, S. Dunaganb, D. Kunsmanb, B. Rutt and U. Catalyurekc, "Dynamic generation of accident progression event trees," *Nuclear Engineering and Design,* vol. 238, p. 3457–3467, 2008.

[11] A. Hakobyan, R. Denning, T. Aldemir, S. Dunagan and D. Kunsman, " A Methodology for Generating Dynamic Accident Progression Event Trees for Level 2 PRA," *PHYSOR,* vol. B034, pp. 1-9, 2006.

[12] I. Årstad and T. Aven, "Managing major accident risk: Concerns about complacency and complexity in practice," *Safety Science,* pp. 114-121, 2017.

[13] J. Rasmussen, "Risk Management in a Dynamic Society: A Modelling Problem," *Safety Science,* vol. 27, no. 2/3, pp. 183-213, 1997.

[14] E. H. Schein, "Culture: The Missing Concept in Organization Studies," *Administrative Science Quarterly,* vol. 41, pp. 229-240, 1996.

[15] U. NRC, "Spent Fuel Transportation Risk Assessment," United States Nuclear Regulatory Commission, Rockville, 2014.

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

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

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

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

[20] 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.

[21] W. Weaver, "Science and Complexity," *American Scientist,* vol. 36, no. 4, pp. 536-544, 1948.

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

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