Advancement of Dynamic Assessment Methodologies for Transportation Security

Adam D. Williams[1], Doug Osborn[1], Brian Cohn[1]

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

Combining dynamic assessment techniques continues to yield new, useful insights for the increasingly complex challenge of securing nuclear transportation. Recent proposals to expand nuclear fuel cycle (NFC) activities are based on nuclear 'fuel take back' arrangements. Such proposals would result in a substantial increase in the quantity and complexity of SNF shipments. The increased quantity in nuclear transportation is clear, but the increased complexity stems from of how international shipments not only require transferring across multiple jurisdictions (at a minimum, those of the shipping and receiving states), but also may require multiple modes of transportation, e.g. rail to water. Such increased complexities challenge traditional approaches to securing nuclear transportation, where a single state shoulders the burden of performing and securing a shipment for its full duration.

In order to capture this increased dynamism and complexity impacting nuclear transportation security, there is a need to develop new assessment approaches. For example, recent research out of Sandia National Laboratories (Sandia) demonstrated how to integrate safety, security, and safeguards for spent nuclear fuel transportation by linking various analysis tools into a single dynamic assessment modeling/simulation (mod/sim) approach. The insights and lessons learned from this research suggest that this same novel approach for transportation security should consider the integration of current assessment techniques with state-of-the-art analytical capabilities. More specifically, this research suggested that linking aspects of various risk-informed approaches, such as system theoretic process analysis (STPA) with dynamic probabilistic risk assessment (DPRA) analysis could enhance current transportation security assessment techniques.

This paper summarizes the conceptual background for—and past experiences in—integrating multiple analysis techniques under a risk-informed, systems-theoretic framework. Using these insights, the paper then describes a dynamic assessment technique for nuclear transportation security based on STPA and DPRA. Then, the data from the hypothetical case (and associated scenarios) are evaluated to demonstrate the benefits of such dynamic assessment approaches. These arguments suggest that a dynamic assessment approach can better capture the complexity, and dynamism experienced in nuclear transportation security—including the ability to reprioritize transportation-related decisions to balance budgetary, geopolitical, and technical challenges.

Background

Sandia National Laboratories (SNL) recently concluded a Laboratory Directed Research and Development (LDRD) project to explore and evaluate risk complexity in nuclear fuel cycle (NFC) activities. This LDRD research demonstrated methodologies for the evaluation of complex risk—including safety, security, safeguards, and *their interactions*—during the international

***SAND2019-5842 C.** 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.*

transportation of spent nuclear fuel (SNF). More specifically, this research considered the changes to the risk profile that arise from multiple modes of transportation and/or jurisdictional and oversight entities [1].

To most accurately capture as comprehensive a picture of "realistic" nuclear transportation security challenges as possible, this research developed a hypothetical case description that is representative of the actual characteristics for an SNF shipping campaign—including identifying various attributes related to transportation security—as possible (see the "Case Study" section, below). This approach allows the use of realistic data sets without identifying "real" vulnerabilities, hazards, or geopolitically embarrassing shortcomings. The resulting hypothetical case study (and set of scenarios) provided the data that served as the foundation for identifying the requirements for a dynamic risk assessment approach for transportation security.

Subsequent research at Sandia has further evaluated the applicability of this dynamic risk assessment approach to other NFC activities. For example, when this dynamic risk assessment was applied to small modular reactors (SMR), the Sandia research concluded that interdependencies between safety, safeguards, and security helped identify leverage points that could increase the efficiency of reactor operations. In specific regards to security, applying this approach to SMRs concluded that passive safety systems *may* represent a new target and set of potential adversary pathways to sabotage SMR facilities [2]. Similarly, ongoing application of this dynamic risk approach to portable nuclear reactors—similar to Russia's floating nuclear reactor [3]—are yielding similarly useful insights to improve security analysis and design for new NFC activities in increasingly complex operational environments. Though focused on demonstrating the benefits of an integrated safety, security, and safeguards approach to address increasing risk complexity across the NFC, the security-specific insights from each such study suggest the opportunity to use similar state-of-the-art analytical capabilities to improve nuclear transportation security.

This growing Sandia research area is based on two state-of-the-art analysis techniques: dynamic probabilistic risk assessment (DPRA) and systems-theoretic process analysis (STPA). The first, DPRA, systematically examines a given scenario as it evolves from initial conditions to a range of possible end states. By explicitly handling the physics- and simulation-based uncertainty points, DPRA incorporates more elements of risk complexity. The second, STPA, creates a representation of the interactions between organizational structures and physical processes. Through the examination of these relationships, STPA identifies the conditions for possibly hazardous states.

Dynamic Probabilistic Risk Assessment (DPRA)

Event trees and fault trees have found great success in examining the uncertainties of systems for safety assessment using static methods. However, traditional event tree approaches require assuming the order of events within a scenario which, when creating an integrated safety, security, and safeguards (3S) analysis, may not be applicable. The timing of events within a 3S scenario may contain uncertainties sufficient to change the order of events in a manner that has a substantial effect on the evolution of (or, security performance within) the scenario. DPRA was created to account for this possibility [4]. Instead of using static event trees and fault trees, DPRA creates

deterministic models to represent the state of the system as a whole and tracks the system evolution during a scenario. This technique is a "bottom up" approach that performs statistical sampling of uncertainties in the deterministic model. The model evolution, incorporating the sampled uncertainties, is tracked to create run-based data and generate insights about risk. For example, the time necessary for offsite local law enforcement officers to arrive at a site in an event requiring a response can play a substantial role in the progression of ensuring steps in the event. If local law enforcement arrives quickly (e.g., before any transport security escorts are killed), then the combined security response forces are much more likely to deter or neutralize adversaries.

The most common family of DPRA techniques is dynamic event tree (DET) analysis, which are similar to event trees in that they begin with one initial state and branch as the scenario progresses in order to cover the uncertainty space. However, unlike traditional event trees, the structure of a DET is not preset and the instead branching occurs at prespecified events during the scenario's evolution. At these points, the logic governing the branching condition determines the number of child branches, the probabilities of each branch and the changes to the system that result. The process is repeated until all branches reach their end state, producing a completed event tree. The resulting DET then is solved following well-established event tree analysis processes. The use of branching conditions rather than a preset structure allows for a higher fidelity examination of the scenario, as well as enabling the examination of the uncertainty space to be systematic, explicitly highlighting the treatment of the modeled uncertainties.

Systems-Theoretic Process Analysis (STPA)

Built on a causality model for complex systems composed of interrelated components maintaining dynamic equilibrium through information and control feedback loops, STPA combines the concepts of hierarchy, emergence, control, and communication into a new paradigm for understanding emergent system properties. STPA, then, evaluates emergent system properties—safety and security, for example—as losses resulting flawed interactions between physical components, engineering activities, operational missions, organizational structures and social factors [4]. This new approach also argues that desired behaviors of complex systems can be redefined as the system's ability to prevent from migrating into states of increased risk (e.g., aspects under the system's control) and experiencing detrimental external events (e.g., aspects *not* under the system's control). For example, this approach would argue that the 2012 security incident at the Y-12 National Security Complex in the U.S. resulted from a degraded security enterprise (e.g., the facility was a state of increased security risk) and the intentional actions of several protestors (e.g., a detrimental external event) [5]. This approach shifts the analytical paradigm from preventing failures to enforcing system constraints and emphasizes three fundamental concepts to eliminate, minimize, or mitigate states of increased risk: constraints (or set points describing hierarchical levels of control), control structures (or, hierarchical socio-technical system models based on accurate and timely communication), and, process models (or, a "mental map" or digital abstraction of the current system state, variables, and processes) [4].

As an analysis technique, STPA identifies undesired system states across technical (physical and cyber) system elements; component interactions; cognitively complex human decision-making errors; and social, organizational, and management factors related to the system. STPA is a "top-down" analysis 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. While STPA does not rank or prioritize these identified hazards, it does provide additional information on which to implement technologies and create protocols to allow complex systems to operate free from unacceptable losses. More specifically, STPA identifies potential inadequate control actions that could lead to a hazardous state, which can result when [6]:

- Unsafe control commands are issued;
- Required safety control actions are not issued;
- Correct safety control actions are provided too early, too late, or in the wrong order; or,
- Control actions are stopped too soon/late, causing inadequate enforcement of safety constraints.

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), STPA identifies undesired system states across by exploring how requirements and desired actions interact to either mitigate or potentially increase states of risk that can lead to unacceptable losses. Because STPA identifies several different causal scenarios for each logical category of control action violation, there is the potential for a smaller number of corrected control actions to eliminate *multiple* causal scenarios for a hazard—including those missed by traditional hazard analysis techniques.

While originally developed for safety analysis (and applied to the aviation, medical, space, and nuclear power domains), STPA is also increasingly being used for security analysis. Here, Young [7] concluded that STPA provides a rigorous, structured problem-framing process, inclusive of a wider range of underlying technical and operational influences on real systems and Williams [8] demonstrated the ability of STPA to refocus port security improvement efforts away from concentric layers of security and toward controllable security control actions. Similarly, recent work in critical infrastructure [9], cyber [10], and nuclear security [11] has argued that the theoretical foundation of STAMP and STPA is highly suitable for security applications.

Case Study

For demonstration purposes, a hypothetical set of countries, material characteristics, and technologies was created to explore the complex risks of SNF transportation.[1] In this example (illustrated in Fig. 1), SNF is physical transported 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 and 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:

[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 [1].

- SNF cask loaded at origin facility (Site A) onto a rail car to the Port of Zamau (grey line);
- SNF cask is transferred from the rail car to a barge at Port of Zamau;
- SNF cask travels via international waters to the Port of Famunda (curved blue line);
- SNF is transferred from the barge to a truck at Port of Famunda;
- SNF cask travels by truck to the Famunda/Kaznirra border crossing (straight orange line); and
- SNF travels by truck to the destination facility (Site B) in Kaznirra (curved orange line).

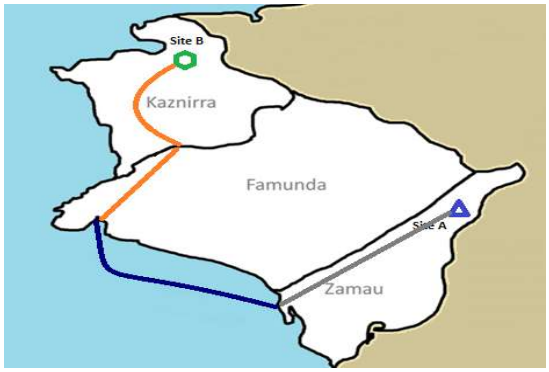

Figure 1. Map and Route of Hypothetical SNF Transportation

The evaluated scenario described how during transit through Zamau, the train encountered a 40 foot stretch of missing track, is derailed, and attacked by a state actor posting as a terrorist organization. If the attack is thwarted, the SNF cask is inspected and then either returned to the origin facility in Zamau or continued onwards to Kaznirra. On the other hand, a successful attack results in the diversion of enough assemblies to obtain one significant quantity of Pu before replacing the assemblies with dummies and creating a radiological release by detonating TNT inside the cask. In this event, the remains of the cask will eventually be shipped back to the origin facility in Zamau and the IAEA will be notified. It is assumed that an IAEA inspector will then be sent to inspect the damaged cask. 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). The details within this case description and scenarios of concern 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.

Results

This Sandia research used both DPRA and STPA to analyze security for this hypothetical international SNF transportation scenario from a dynamic risk assessment perspective.[2]

Within the DPRA-based security analysis, DETs explicitly coupled safety, safeguards, and security decisions by building direct links via branching conditions—or predetermined simulation

[2] For complete analytical details, please see [1]

conditions indicating a need to incorporate a key interdependency. As these points can often have conflicting outcomes when analyzed individually, modeling the *interrelated* effects of uncertainties in both directions allows decision-makers to understand the full effects of the modeled uncertainties and systematically capture the entirety of the system space. For example, one branching condition used was the degree of advanced notification given to local law enforcement (LLE) along the SNF transportation route. Advanced LLE notice in this analysis is assumed to cause a more rapid offsite response, due to earlier preparation, and an increased distribution of adversaries, representing the potential for information leaks. Table 1 shows how the probability of neutralization (P_N) is affected by the level of LLE notification for this scenario.

Table 1. P_N based on LLE notification

Scenario	**Average P_N**
Full Scenario	65.91%
Advanced LLE Notice	72.38%
Minimal LLE Notice	59.46%

In addition, DETs can reveal new *interactions* with safety and safeguards that have a significant impact on security. For the derailment scenario, a potentially interesting interaction is the effect of the derailment itself preventing adversary access to the cask. Derailment has the potential to throw up wreckage and ignite fires in the proximity of the cask, which would require time to traverse and have the effect of giving offsite responders more time to arrive. A subset of 96 simulation realizations was considered for this effect; 72 with no assigned time penalty and 24 with a time penalty to the adversaries of 40 seconds. Each run consisted of 8 adversaries and 8 onsite responders. An additional 3 offsite responders arrived after a random time. Adversaries won if they either breached the cask or neutralized all response forces, offsite and onsite, while the response forces could only win by neutralizing all adversaries before they breach the cask.

Table 2. P_N for a subset of runs with assigned time penalty to adversaries based on wreckage from derailment

Time Penalty	
0s	40s
90.3%	100.0%

Table 2 shows P_N for no time delay and a time delay of 40 seconds. The additional time for offsite responders had an effect on P_N. Adversaries defeated the response forces in seven of the 72 runs with no time penalty. In three of these adversary victories, the SNF cask was breached before the adversaries were neutralized by offsite responders. Additionally, in several of the runs where responders won, the adversaries were neutralized in fewer than 10 seconds before the cask would have been breached, highlighting the importance of uncertainties in the timing of adversaries and response forces.

Within the STPA-based security analysis, identified potential violations of control actions described challenges to the physical movement from an origin facility to a destination facility without disruption to selected and approved routes, timelines, and operations from intentional, malicious actions. Identified security-specific states of increased system risk included

unauthorized access of the cask (or the transportation vehicle), transportation vehicle stopped longer than expected, transportation vehicle traveling slower than scheduled, and unverified transfer of armed security responsibility. As shown in Table 3, using STPA these security states of increased risk helped generate both high-level system requirements and related control actions.

Table 3. Representative Set of System Requirements and Associated Control Actions to Mitigate Related States of Increased Risk Security of International SNF Transportation.

Emergent Property	State of Increased Risk	System Requirement	Representative Control Action [Specific Controller]
Security	Unauthorized access of cask*	Unauthorized individuals must not access cask	Engage lid-locking mechanism [Cask]
			Check credentials of inspectors of the cask [Local Law Enforcement Agency]
	Unverified transfer of armed security responsibility	Any transfer of armed security must be verified	Confirm scheduled time for security responsibility transfer [Transportation Security Operations]
			Communicate process for transfer of armed security responsibilities [Competent Authority]

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. For example, evaluating each control action against these four violation criteria results in alternative system states, or possible states of the system predicated upon a specific violation of the related control action. 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 representative security control actions.

Table 4. Representative Set of Security Control Actions, with Both Traditional and 3S STPA Labels, Evaluated in Scenario 1 for International SNF Transportation.

Control action	STPA Label / 3S STPA Label	SIR Identified
Engage rail car immobilization mechanism	SECA1	SIR5, SIR6 (NNP) SIR5, SIR7 (PNN_1)
	3SCA5	SIR5, SIR6 (NNP) SIR5, SIR7 (PNN_1) SIR2 (PNN_2)
Communicate the process for transferring armed security responsibility	SECA2	SIR9 (NNP) SIR7, SIR9 (PNN_1)
	3SCA6	SIR5, SIR9, SIR10 (NNP) SIR5, SIR7, SIR9 (PNN_1)
NNP = "needed, not provided"; PNN = "provided, not needed"; Too early = "provided tool early" Subscripts denote a particular conditional description for a violated control action aligned with a given state of increased		

This STPA analysis showed that interactions with safety and safeguards impact security performance for international SNF transportation. For example, 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 inspector in a country with limited resources).

Implications for a *Combined* Analytical Technique

As demonstrated from the case study, DPRA and STPA consider security risk from different analytical perspectives. DPRA considers security risk arising from failures in physical protection components or from human actions resulting in an unacceptable security end-states. STPA considers security risk to a system based on the state of the control processes and feedback structures. Combining these two perspectives has the potential for creating a more complete picture of the security risk than either approach alone. More specifically, the analytical strengths of one approach *seems* capable of mitigating weaknesses in the other.

The primary strength of DPRA is its ability to provide quantitative descriptions of security risk, which provides the foundation for security risk prioritization. Conversely, DPRA's primary weaknesses relates to formulating scenarios. DPRA analysis provides little information on how to construct scenarios, specifically with regards to what components, systems, and uncertainties should be included to ensure a full picture of a system. Though sensitivity studies are used to determine the necessity of obtaining uncertainty information, DPRA also struggles to provide the analyst with specific information regarding what elements within a scenario are uncertain and need to have their uncertainty distributions identified. As a result, DPRA struggles to identify *new* or *non-traditional* failure modes within systems.

The primary strengths of STPA, on the other hand, are its scenario generation and ability to more fully identify hazards (or, in DPRA terms, new and non-traditional failure modes). The primary weakness in STPA, however, is its lack of prioritizing the fuller set of identified hazards. STPA is capable of systematically identifying which lapses in control actions can lead to hazardous states, as well as what scenarios can result from these hazardous states. Yet, STPA provides no method of quantifying these hazards, either by determining the probabilities of entering the predicted hazardous states or of the negative outcomes arising from the predicted scenarios.

Comparing these strengths and weaknesses suggests the potential for combining DPRA and STPA, enabling the logical prioritization of the former leverage the robust scenario generation of the latter. This *Dynamic System Theoretic and Probabilistic Analysis* (DSTPA) process would begin by using STPA to rigorously and systematically identify hazards and hazardous control actions for the system. These hazardous control actions help generate scenarios can then be evaluated with DPRA to determine the probabilities and consequences of various outcomes. These quantitatively described outcomes are mappable to the reliability of individual components/systems as well as violations of control actions that impact system-level (e.g., emergent) behaviors. If deemed unacceptable, the identified risks can be reduced by (1) altering the components/systems involved

to add additional redundancy or increase system reliability (traditional DPRA); (2) improving enforcement of control actions to generate desired system behaviors (traditional STPA); or, (3) a combination of the two.

For example, reconsider the hypothetical case where SNF is being transported from a reactor to a storage site by rail. The results of the STPA would conclude that if control actions related to railway integrity are violated, the SNF shipment could suffer a derailment. (Again, note that the cause of railway damage is not specified in STPA, so it could be natural degradation *or* intentional.) DPRA would then be performed for these different scenarios to determine the probabilities and consequences of these events. Being able to compare these scenarios improves transportation security risk management and helps identify a range of potential measures for improving security. Such measures could include: further strengthening the cask, increasing the number of security escorts for the SNF, implementing preventive railway maintenance, or changing the hierarchical governance structure to separate the duties of rail inspection and maintenance from the shipping entity—each of which would reduce the consequences predicted by DPRA built on scenarios generated from STPA. A DSTPA-type approach would also allow for better evaluating the transportation security risk reduction from a *completely different* transportation, like transporting the SNF by road and thus replacing the security risks with rail transportation with those associated with roads.

Conclusions

Trends and dynamics predicted for future nuclear shipping campaigns suggest they will be more complex than the current transportation system is prepared to handle. Related security challenges include greater international transportation of nuclear materials across jurisdictions and more transportation by smaller countries or commercial entities who may be unable (or unwilling) to shoulder all security responsibilities for the transportation campaigns. An additional challenge stems from the potentially contradictory recommendations from safety and security analysis. Finally, shipments requiring multiple modes of transportation will generate more complexity—particularly in regards to maintaining consistent (and adequate) security—at transfer points.

Both the DPRA and STPA thrusts demonstrated the ability to integrate safety and security analyses to provide a more complete picture of this increasing risk complexity. Traditional safety and security analyses are conducted independently, resulting in recommendations that may be contradictory or overlapping—and provides no way to gain a simultaneous understanding of the interdependencies, gaps, or leverage points. For example, in the case study, the effects of providing advanced notification of shipments was examined which allowed the analysis to simultaneously explore the interdependent effects of advanced notification (e.g., it enhances safety but challenges the "need to know" concept of security) on overall transportation security risk. Such insights suggest a dynamic assessment approach—perhaps similar to the DSTPA idea introduced in the previous section—can better capture the risk complexity experienced in nuclear transportation security. Dynamic assessments, then, include the ability to reprioritize, optimize, and redesign transportation security-related decisions to balance budgetary, geopolitical, and technical challenges.

References

[1] A. D. Williams, D. M. Osborn, K. A. Jones, E. A. Kalinina, B. Cohn, A. H. Mohagheghi, M. DeMenno, M. Thomas, M. J. Parks, E. Parks and B. Jeantete, "System Theoretic Fremeworks for Mitigating Risk Complexity in the Nuclear Fuel Cycle (SAND2017-10243)," Sandia National Laboratories, Albuquerque, 2017.

[2] A. D. Williams, D. M. Osborn and B. Cohn, "System Studies for Global Nuclear Assurance & Security: 3S Risk Analysis for Small Modular Reactors (Volume II)-Conclusions & Implications (SAND2018-14164)," Sandia National Laboratories, Albuquerque, 2018.

[3] International Atomic Energy Agency, "KLT-40S Overview," International Atomic ENergy Agency, Vienna, 2013.

[4] T. Aldemir, "A Survey of Dynamic Methodologies for Probabilistic Safety Assessment of Nuclear Power Plants," *Annals of Nuclear Energy,* vol. 53, pp. 113-124, 2013.

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

[6] G. Friedman, "Inquiry into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex," U.S. Department of Energy, Washington, DC, 2012.

[7] N. Leveson and J. Thomas, STPA Handbook, Cambridge: MIT Press, 2018.

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

[9] 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.

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

[11] W. Young, *A System-Theoretic Security Analysis Mthodology for Assuring COmplex Operations Against Cyber Disruptions,* Cambridge: Massachussets Institute of Technology, Dissertation, 2015.

[12] A. D. Williams, "System Security: Rethinking Security for Facilities with Nuclear Materials," *Transactions of the AMerican Nuclear Society,* vol. 109, no. 1, pp. 1946-1947, 2014.