CN-244-310 SAND2016-11712C

A New Look at Transportation Security: A Complex Risk Mitigation Framework for the Security of International Spent Nuclear Fuel Transportation

A.D. Williams[1], D.M. Osborn[1], K.A. Jones[1], E.A. Kalinina[1], B. Cohn[1], M.J Parks[1], E.R. Parks[1], E.S. Johnson[1], Amir H. Mohagheghi[1]

[1]Sandia National Laboratories*, Albuquerque, New Mexico, U.S.

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

Abstract. Growing interest in nuclear energy programs worldwide and the high cost of managing spent nuclear fuel (SNF) introduces additional complexity into traditional nuclear material transportation operations. New elements of complexity facing securing such transports include, but are not limited to:

- an increasing number of SNF cask transfers between transportation modes (e.g., road to rail to water);
- an increasing number of geopolitical or maritime borders crossed by SNF casks; and,
- the higher potential for inconsistent security requirements, resources and regulations along approved international SNF transportation routes.

Combining the expected increase in SNF shipments with the emergence of multimodal transportation routes illustrates increases in risk complexity for SNF transportation. Further, this increase in risk complexity directly challenges traditional approaches to SNF transportation security that build off of decades of transportation safety analyses, which themselves are derived from technical cask design, acceptable dose rates, defense-in-depth strategies and probabilistic hazard estimates. Recent work in risk mitigation and SNF transportation studies suggest that applying a complex risk mitigation perspective built on the interdependence of security, safety and safeguards can improve the security design and analysis of international SNF transportation.[1] More specifically, such a paradigm shift helps identify solutions more aligned with complex realities and potential real world hazards than traditional approaches driven by safety regulations determined from SNF cask degradation laboratory experiments.

The evaluation of two novel, system-level analysis techniques against a hypothetical, international SNF transportation case demonstrates such benefits. First, dynamic probabilistic risk assessment (DPRA) builds on traditional probabilistic-based methods to provide a unified framework to account for the joint effects of aleatory and epistemic uncertainties on SNF transportation risk to provide a more complete set of identified event sequences leading to undesirable consequences. Similarly, system theoretic process analysis (STPA) combines the concepts of hierarchy, emergence, control, and communication to model SNF transportation as a complex socio-technical system where system-level risk is managed by ensuring the control of interactions between technologies, organizational influences and environmental pressures.

The paper will discuss how an integrated complex risk mitigation framework offers several benefits to reducing security vulnerabilities to the expected increase in international SNF shipments in the near future. In addition to expanding the solution space for transportation security, this framework also provides opportunities to enhance safeguards on SNF in transit as well as options to increase coordination between security, safeguards and safety—ultimately mitigating and managing the increasingly complex risks from the international transportation of SNF.

Key Words: Transportation security; Complex risk; Integrated 3S; Risk management.

* 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. **Programmatic Review**

1. Introduction

Whether spawning from spent nuclear fuel (SNF) reclamation projects (e.g. estimates of more than 12,000 shipments of SNF are expected by 2055 in the U.S. alone [2]) or the increasing popularity of commercial nuclear 'fuel take back' agreements, the expected result is a significant increase in the amount of SNF to be transported around world. Growing interest in nuclear energy programs worldwide and the high financial and political cost of managing spent nuclear fuel (SNF) have introduced increased complexity into traditional nuclear material transportation operations. New sources of complexity for the security of SNF transportation include, but are not limited to:

- an increasing number of SNF cask transfers between transportation modes (e.g., road to rail to water);
- an increasing number of geopolitical or maritime borders crossed by SNF casks;
- the higher potential for interactions with safeguards and safety to affect SNF transportation security;
- the higher potential for inconsistent security requirements, resources and regulations along approved international SNF transportation routes; and,
- the increased salience of regional and geopolitical issues for framing a dynamic threat environment along approved international SNF transportation routes.

Individually, any of these sources challenge traditional approaches to designing and evaluating transportation security that build off of decades of SNF safety analysis, which are a function of technical cask design (e.g., physical vessel containing the SNF assemblies), acceptable dose rates, defense-in-depth systems and probabilistic hazard estimates. Taken together, they represent a significant increase in complexity facing secure SNF transportation and suggest the need for new analytical approaches. Recent work in risk mitigation [3] and SNF transportation studies suggest that applying a complex risk mitigation perspective built on the interdependence of security, safety and safeguards can improve the security design and analysis of international SNF transportation.[1] This paper hypothesizes that considering SNF transportation security as part of an integrated complex risk management framework provides higher fidelity analysis of potential real world hazards and helps identify solutions more aligned with complex realities than traditional approaches that isolate security analysis for SNF transportation.

Invoking a broader concept and socio-technical context for risk offers a new paradigm for incorporating such variables as the integrity of security components during transportation mode changes; potential degradation of security component performance under different operational or geopolitical contexts; appropriateness of security components for dynamically changing threat environments; and, interactions with elements and procedures to enhance safety (e.g., cask integrity and speed of transport vehicle) and safeguards (e.g., real-time location tracking and seals). Building on prior theoretical studies ([4], [5], [6]), Sandia National Laboratories (SNL) suggests that modeling SNF transportation as a complex, socio-technical system is better able to manage the associated complex risk—including improvements in security—in international environments.[1] In this analytical framework, security is considered a key characteristic of a complex risk metric that accounts for the challenges to international SNF transportation related to malevolent access to the SNF for theft or sabotage purposes. This paper will use a hypothetical case study to introduce two new, novel analysis techniques—dynamic probabilistic risk assessment (DPRA) and system theoretic process analysis (STPA)—to support this complex risk perspective of security and demonstrate its benefits over traditional approaches.

2. Case Study[1]

[**NOTE:** The case description draws from a wide range of publically available reports and articles detailing SNF (specifically) and special nuclear material (SNM) transportation cases (more generally). The goal of the description is to provide a realistic, detailed case study—inclusive of the many sources of risk complexity described in the literature—for development of a socio-technical system and risk management analytical framework.]

The country of Zamau has been using nuclear power for 48 years, and has exceeded the storage capacity available onsite for their fuel. In two years, they plan to begin shipments to the nation of Kaznirra, which has an economic incentive to receive SNF from surrounding countries.

While Zamau has executed some in-country transportation of SNF in the past, it has not historically participated in regional shipments. Kaznirra has received SNF from one other nation as part of its efforts to establish itself as a central storage location for the area, but those shipments only involved a single border crossing and one mode of transportation (truck).

The geopolitical situation in the region is similar to that of east African countries, with instability and some strong insurgent groups in the area, as well as state-level corruption in several cases. The greatest instability along the transportation route is in the country of Famunda, which is between Zamau and Kaznirra. The region and route are shown in Figure 1.

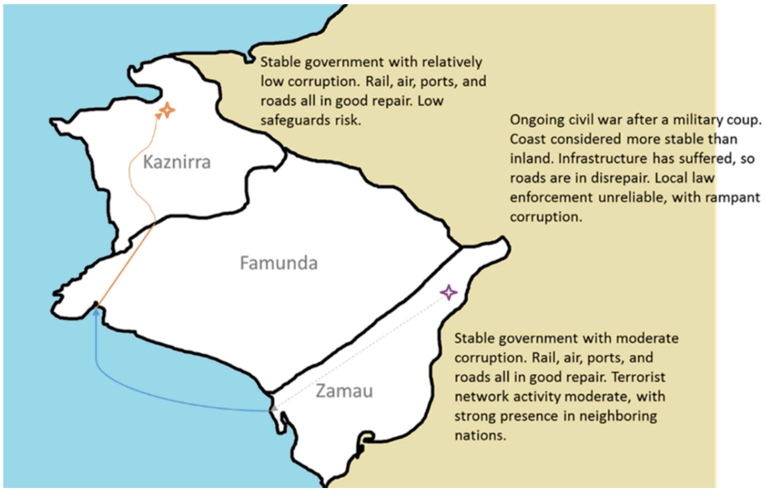
Stable government with relatively low corruption. Rail, air, ports, and roads all in good repair. Low safeguards risk.
Ongoing civil war after a military coup. Coast considered more stable than inland. Infrastructure has suffered, so roads are in disrepair. Local law enforcement unreliable, with rampant corruption.
Kaznirra
Famunda
Zamau
Stable government with moderate corruption. Rail, air, ports, and roads all in good repair. Terrorist network activity moderate, with strong presence in neighboring nations.

Figure 1. A Notional Region and Route for the Transport Scenario

Kaznirra is a parliamentary republic with five provinces and a president who serves as head of government. It has 20,000 km of railway, but its roadways are about 65% unpaved. Military units are often need to be placed along the border to control poaching and drug smuggling. Kaznirra does have a well-developed nuclear enterprise (including being a non-

[1] The notional countries within this hypothetical case description are loosely based on real countries for the purpose of borrowing realistic descriptions of infrastructure condition, climate, and political/security considerations. They are not intended to represent a real-world route under consideration, and other assumptions (such as history of nuclear power use) for each notional country may be based on another nation's historical information.

weapons state signatory to the *Treaty on the Non-Proliferation of* Nuclear *Weapons* (NPT), signing the Additional Protocol (AP) and being a Nuclear Suppliers Group (NSG) member) that provides approximately 5% of the nation's electrical power and includes the SNF storage facility. To date, there have been no reported attempts to breach Kaznirran nuclear facilities or transports. The border security officers are instructed to prioritize protecting the border (e.g., counter drug smuggling) over assisting in the security of any shipment (including SNF) temporarily held onsite.

Famunda is a presidential republic with a President, a Prime Minister, and a Council of Ministers appointed by the president. The President is elected via a majority popular vote. The legislative branch is a National Assembly with 255 seats. Both urban and rural roads in Famunda are 90% unpaved and there is only one major seaport. Famunda is often used as a narcotics transshipment point, although the increasing political instability in the country has made it less favorable to cartels. Rampant corruption exists and the financial system is considered undeveloped. Famunda has no electricity from nuclear plants, so they do not have a developed safeguards system, but they have signed the NPT as a non-nuclear weapons state.

Zamau is a presidential republic with a mixed (e.g., common and customary law) legal system. Civil wars in Zamau resulted in a recently completed UN peacekeeping mission and moderate levels of corruption and terrorist network activity in-country and along its borders. Zamau has 5,000 km of railways, with the most usable running from near a national SNF collection site to a port on the coast. The roadways in Zamau are about 15% unpaved and the country boasts one strong port facility. Military units are used along the border to control poaching and the smuggling of illicit drugs, people and terrorists. Zamau boasts a fairly robust nuclear enterprise, including hosting several facilities generating SNF that provides approximately 12% of Zamau's electrical power and is a non-weapons state NPT signatory. There have been a growing number of low-level labor disputes by contract-based security forces and a few rumored (and unconfirmed by the government) attempts to breach Zamuan nuclear facilities.

The SNF generated in Zamau consists of 50 GWd/tU[2] fuel rods removed from a pressurized water reactor that has been sitting in wet storage at Site A for up to 50 years. As such, this SNF will be transported in an IAEA-compliant, type B cask (e.g., similar to the AREVA TN cask series, [7]). The overall goal of this case is for this SNF to travel from a storage site in Zamau (Site A) to the disposal site in Kazmirra (Site B), according to this high level route description:

- SNF cask is loaded from the storage site (Site A) in Zamau onto a rail car for transporation to the Port of Zamau where it is loaded onto a barge;
- SNF cask travels via international waters to the Port of Famunda in the southwest corner of the country and loaded onto a truck; and,
- SNF cask travels by road through western Famunda, across the border and across interior Kaznirra to Site B.

This hypothetical route was selected amidst a set of security-related factors[3], including the desire to avoid the greater political instability and terrorist activity of interior Famunda and

[2] These units, Gigawatt-days per ton of enriched uranium, is a descriptor of how nuclear material is used within a given power reactor.

[3] For more details on the associated analytical assumptions—and their justification—please contact the main author.

along Kaznirran borders. There are also various types of inspections along the route (e.g., Zamaun national safety inspections upon cask loading or manifest comparison at the Port of Famunda) that demonstrate the additional complexities introduced by inconsistent regulations—and the potential for resulting lapses of security along international routes.

3. Complex Risk Approaches to SNF Transportation Security

Dynamic probabilistic risk assessment (DPRA) provides a 'bottom-up' framework for evaluating complex risk from an integrated 3S perspective. Developed in response to challenges to conventional event-tree/fault-tree methodologies, DPRA uses dynamic event trees (DET) to better account for real-life uncertainties.[8] DETs provide systematic and automated assessment of possible scenarios arising from uncertainties in complex systems [9] and allows for a systematic, automated and integrated 3S analysis.[1] DPRA employs DET models for a seamless transition from a safety-to-security-to-safeguards analysis inclusive of a two-loop process to evaluate epistemic (e.g., arising from the model) and aleatory (e.g., arising from stochasticity of the processes) uncertainties in a systematic and coherent fashion.

Moreover, the Analysis of Dynamic Accident Progression Trees (ADAPT) software is used for generating the DETs for the DPRA approach to integrated 3S complex risk analysis.[1, 9] ADAPT acts a controller and scheduler of possible scenarios based on the branching and stopping rules determined by varying uncertainty parameters, as well as technical and social variable values. ADAPT graphically displays the DETs (and scenario likelihoods) as a function of time and provides a mechanism for addressing the 3S interdependencies by linking traditional security, safety and safeguards risk analysis codes[4] in a novel manner. Within the DPRA framework, security is evaluated as an individual characteristic of complex risk influenced by (and influencing) the risk associated with the safety and safeguards of SNF during international transportation. These influences are dynamically inserted (and propagated) through the DETs along a particular attack path of concern. Security, then, is re-cast as a stochastic description of risk associated with malicious intent by adversaries within an environment framed by a higher fidelity representation of aleatory and epistemic uncertainty.

Similarly, the system theoretic process analysis (STPA) argues that managing the complex risk of international SNF transportation can be seen as eliminating, minimizing or mitigating migration into states of higher risk.[10] Modeling SNF transportation as a complex, socio-technical system, STPA is a top-down analytical technique that provides a rigorous, structured mechanism for linking specific design details to supporting overall system (e.g., security, safety and safeguards) objectives.[1] By defining risk as a system state, STPA describes behaviors that influence risk (e.g., security) emerging from the interaction of the components within the system. Treating security in this manner provides a traceable, non-probabilistic (e.g., described as plausible loss of control, not stochastic estimate of frequency) framework by which to compare proposed measures to improve the complex risk mitigation of international SNF transportation.

[4] For security, STAGE (a SNL-specific application of a commercial code that uses logic based behavior models and its artificial intelligence to simulate complex behaviors, intelligent reactions and dynamic path planning on a flexible platform) is used [11][12], for safety, RADTRAN (an internationally accepted program and code for calculating the risks of transporting radioactive materials) is used [13] and for safeguards, PR-CALC (a novel Markov molding approach that quantitative describes proliferation resistance as state transitions) is used [14].

STPA uses hierarchical control structures and functional control loops to model complex systems. Control actions provided by higher levels in a hierarchical control structure limit the behaviors of lower levels, and the process of control action issuance, implementation and feedback is modeled with a control loop. STPA then uses control loops to analyze control actions for possible violations that lead to ineffective security (e.g., system states of higher risk) and consists of two major steps [10]:

- '**Step One**': rigorously identify possible violations of control actions that lead to system states of higher risk (including, when incorrect control actions are issued; required control actions are not issued; control actions are provided too early or late; or control actions are stopped too soon (or too late) to be adequately enforced); and,
- '**Step Two**': derive specific scenarios, based on observed or regular system operations, that could cause the theorized control action violations to occur.

In an STPA analysis, security is described as the ability to control technical (e.g., advanced SNF cask lock) and social (e.g., security inspection procedures) component interactions to mitigate migration of the system to a state of higher risk. Rather than quantifying the reliability of such components against anticipated adversary capabilities (like DPRA), STPA treats security as the ability to maintain control of security components within desired operational limits. In addition, STPA argues that a 3S redefinition of SNF transportation complex risk helps identify requirements and control actions to enforce that will avoid system states of higher (or unnecessary) risk.[1] Further, in the STPA approach to integrated 3S complex risk analysis, control of these security requirements and control actions are also influenced by (and influence) safety and safeguards efforts—ultimately offering a higher fidelity description of the operating environment for transportation security.

Both DPRA and STPA complex risk analysis frameworks suggest potential benefits for improving security of international SNF transportation over traditional approaches. Table 1, below, summarizes the key attributes of each approach.

Table 1. Summary of key attributes of two complex risk approaches related to security

Key Attribute	DPRA	STPA
Risk characterization	Stochastic description of likelihood of undesired events	Level of control to prevent system migration into a state of higher risk
Type of Uncertainty	Aleatory, Epistemic	Coordination, Heuristics, Biases
Type of Complexity	Combinatorial, Dynamic	Dynamic, Interactive
Influence on Security	Probabilistic description(s) of security component reliability along path(s) framed in complex risk uncertainty	Technical (reliability), organizational & (threat) environmental interdependence & feedback
'Direction' of Analysis	Bottom-up	Top-down

4. Analysis & Discussion

To focus the scope of the analysis, prior SNF transportation analyses were surveyed to identify a useful, representative set of specific scenarios of concern. These prior studies emphasized cask survivability against a range of traditional adversary attack paths (e.g., direct kinetic attack on the cask) but did not account for possible theft of the SNF in transit or an insider conspiracy to hijack the transportation vehicle—let alone geopolitical or organizational influences on efforts to improve security along a route. These types of security influences were included in the scenarios selected for this analysis given their hypothesized increase in salience on SNF transportation. As such, the following scenario related to the hypothetical international SNF transportation case description was selected for this paper:

- Scenario: the transfer of security responsibilities between officials when the SNF transportation truck crosses the Famunda/Kaznirra border. Because of the ongoing civil unrest in Famunda, the Kaznirran government has established a lengthy SNF responsibility transition process that includes more detailed SNF vehicle and cask inspections, as well as approval from several Kaznirran federal government offices (including the competent security authority). On average, this approval process takes 24 hours to complete—therefore, the SNF transportation vehicle is left in the vehicle arresting area overnight. During this process, the armed Famunda security personnel who escorted the SNF transport vehicle through Famunda are housed in the guard barracks until they are officially relieved of their security responsibilities by Kaznirran security personnel.

Here, the scenario description includes insights provided by the World Nuclear Transport Institute (WNTI) and the World Institute for Nuclear Security (WINS)—specifically the importance of coordination of security responsibilities between entities along the route and at points of transfer.[15] Further, this scenario was partially motivated by an Indonesian case in which

> Coordination was focused on the security plan for land and see transportation of SNF. On land security it was coordinated by Regional Police of Banten, Jaw Barat, DKI, Yogyakarta and JawTengah provinces. Security for sea transportation was coordinated by RI [Royal Indonesian] Navy.[16, p.113]

This scenario demonstrates a need for SNF transportation security analysis approaches that can incorporate social and organizational influences related to coordinating security continuity across regional, and within national, entities. Both DPRA and STPA are used to evaluate this scenario of the hypothetical international SNF transportation case description provided in the earlier section.

DPRA complex risk analysis propagates non-traditional influences (e.g., the need for Kaznirra to confirm safeguards integrity after transit through a country without international safeguards agreements) through DETs to offer a more realistic description of the security environment at the Famunda/Kaznirra border. Similarly, DETs captures uncertainties associated with these non-traditional influences—including the estimated time for Kaznirra to officially take responsibility of the SNF after it arrives (aleatory) and its mathematical representation as a related probability distribution (epistemic). Consider, more precisely, how this unknown time for Kaznirran approvals can result in confusion between which force holds security responsibility while the SNF transport is in the arresting area at the Kaznirra/Famunda border. Such confusion (which is not considered in traditional approaches) could result in uncoordinated (at best) or delayed (at worst) response to an adversary attack—increasing the probability of a successful adversary attack on the SNF.

In addition, including the interdependent consequences (e.g., radiological dispersion, loss of material or area contamination) of a 3S DPRA complex risk analysis expands both the problem and solution space for international SNF transportation. An example of the former is explicitly incorporating how the extended Kaznirran process for confirming safeguards credibility influences the aleatory uncertainty relates to the adequate response to an attack on the SNF vehicle while in the border control arresting area. This suggests a need for potential solutions beyond the traditional focus on ‘reducing response force time,’ to including (but not limited to) increased clarity over the precise time of security responsibility transition from Famunda to Kaznirra (established prior to the shipment) and enhanced communication between the two forces (during the shipment). Neither of these solutions to improve security are identified using traditional security analysis techniques.

Similarly, an STPA complex risk analysis describes the security as maintaining control over system behavior against a realistic set of plausible influences working to degrade security effectiveness related to the SNF transport vehicle. For example, Kaznirran efforts to ensure credible safeguards of the SNF, given the lack of a strong Famundan safeguards capability, may result in a possible diversion of resources or attention to ensuring security protocols are adequately followed. Likewise, a regional bias toward ensuring the safety of the SNF during transit represents a geopolitical challenge to the ability to maintain adequate security control. Here, pressures to ensure safety might cause the Famundan security force to travel more slowly along the Famundan road portion of the route—which may increase security risk by violating security inspection timelines or increase the amount of time the SNF transport vehicle is in hostile area.

STPA’s hierarchical control structure model also clearly identifies two additional sources of non-traditional influences on security: coordination and feedback. As described above, the ability of the SNF transport vehicle to be protected against an attack while housed in the border checkpoint arresting area is directly related to the coordination between Kaznirra and Famunda forces. STPA illustrates this potential increase in security risk and helps identify mitigating mechanisms. The emphasis on feedback in the STPA also helps explicitly identify the important—and non-stochastic—role that humans plan in preventing system migration into states of higher security risk (degraded effectiveness). More specifically, this approach links the ability of Kaznirran security forces to adjust their security posture after identifying potentially insufficient security reporting from the Famundan security personnel.

Ultimately, both DPRA and STPA provide complex risk frameworks that better contextualize the traditional (e.g., adversary capabilities) and non-traditional (e.g., environmental, organizational, safety or safeguards interdependencies) influences in the dynamic threat environment facing international SNF transportation. This approach also better characterizes the changing complex risk profile along individual international SNF transportation routes. This also suggests that considering security as an interdependent characteristic of complex risk provides a larger problem and solution space.

5. Conclusions

As demonstrated above, there are a number of benefits in evaluating security as a key characteristic of complex risk and from a socio-technical, risk management perspective, which are summarized in Table 2 below. For example, the Kaznirra/Famunda border scenario necessitates the official transition of security responsibility between two sovereign nations. The potential increases in security risk (e.g., delayed or ineffectual response) are not explicitly included in traditional approaches to nuclear transportation security. This organizational complication is one of many expected to increase in frequency with the expected increase in international SNF transportation as the current model of one country providing start-to-finish protection and oversight of nuclear material transportation (e.g., the U.S.-sponsored efforts to remove highly enriched uranium for civilian research reactors around the world) becomes untenable. A complex risk framework can also identify non-traditional influences the might increase security risk that are outside the analytical scope of traditional approaches.

Table 2. Summary comparison of traditional vs. complex risk characterization of security

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

Moreover, evaluating security improvement from a risk management trade-space perspective can better manage the complex risk facing international SNF transportation than reducing security risk in isolation. In addition to expanding the solution space for transportation security alone, this framework also provides opportunities to enhance safeguards on SNF in transit and options to increase coordination between security, safeguards and safety—ultimately mitigating and managing the increasingly complex risks from the international transportation of SNF.

6. References

[1] WILLIAMS, A., et. al., “Preliminary Results from a System-Theoretic Framework for Mitigating Complex Risks in International Transport of Spent Nuclear Fuel”, INMM 2016, (Proc. Annual Mttg. Atlanta, GA., 2016).

[2] KALININA, E., et. al., “Transportation of Spent Nuclear Fuel from Reactor Sites in the US—What Will it Take?”, IHLRWM 2015 (Proc. of ANS Inter’l Conf., Charleston, SC, 2015).

[3] GARBOLINO, E., et. al., “A simplified approach to risk assessment based on system dynamics: An industrial case study”, Risk Analysis **36(1)** (2016) 16-29.

[4] CIPORALLO, A., LOMONACO, G., “Contributing to the nuclear 3S’s via a methodology aiming at enhancing the synergies between nuclear security and safety”, Progress in Nuclear Energy, **86** (2016) 31-39.

[5] DARBY, J., et. al., Framework for Integrating Safety, Operations, Security, and Safeguards in the Design and Operation of Nuclear Facilities, SAND2007-6429, Sandia National Laboratories, Albuquerque, NM (2007).

[6] MOHAGHEGHI, A., Education Programs for Integrated Nuclear Safeguards, Security, and Safety, IAEA Conference on Managing the Development of a Sustainable National Infrastructure for Nuclear Power Plants (Invited Talk), Vienna (2012).

[7] GARCIA, J., “Dual Purpose Casks in Operation”, IAEA Workshop in the Development and Application of a Safety Case for Dual Purpose Casks for Spent Nuclear Fuel (Presentation), Vienna (2014).

[8] HAKOBYAN, A., et. al., “A Methodology for Generating Dynamic Accident Progression Event Trees for Level 2 PRA”, PHYSOR **B034** (2006), 1-9.

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

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

[11] CIPITI, B., et. al., “Safeguards and security modeling for electrochemical plants”, GLOBAL 2013 (Proc. of Inter’l NFC Conf, 2013) 1598.

[12] DOMINGUEZ, D., et. al., “Special Nuclear material and critical infrastructure security modeling and simulation of physical protection systems”, ICCST 2012, (Proc. IEEE Inter’l Carn. Conf. Boston, MA., 2012).

[13] WEINER, R., et. al., RADTRAN 6/RadCat 6 User Guide, SAND2013-8095, Sandia National Laboratories, Albuquerque, NM (2013).

[14] YUE, M., et. al., “A Markov model approach to proliferation resistance assessment of nuclear energy systems”, Nuclear Technology **162** (2008) 26-44.

[15] WORLD INSTITUDE FOR NUCLEAR SECURITY, WORLD NUCLEAR TRANSPORT INSTITUTE, Nuclear Security Transport: International Best Practice Guide, **4.1**, Vienna (2015).

[16] IMAN, K., et. al., RRSNF Shipment Operation of Indonesian Research Reactors, Return of Research Reactor Spent Fuel to the Country of Origin: Requirements for Technical and

Adminstrative Preparations and National Experiences, (Proc. of IAEATech. Mttg. Vienna 2008) 109-119.