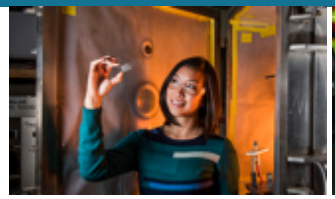
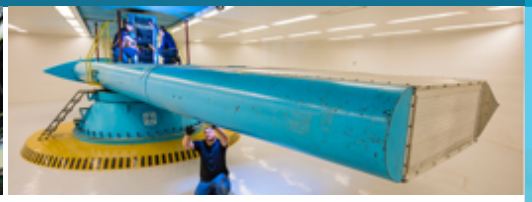
System Theoretic Frameworks for Mitigating Risk Complexity in the International Transportation of Spent Nuclear Fuel





PRESENTED BY

Adam D. Williams, Douglas Osborn, and *Elena Kalinina*

Probabilistic Safety Assessment and Management

PSAM14, September 16-21, 2018, Los Angeles, CA

Outline

- Introduction
- Case Study
  - *International SNF Transportation Hypothetical Case Study*
- Final Results
  - *Dynamic Probabilistic Risk Assessment (DPRA)*
  - *System Theoretic Process Analysis (STPA)*
- Conclusions

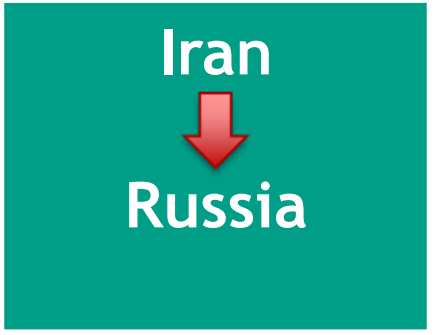
Introduction (I)

New nuclear energy programs and fuel takeback programs suggests a rise in *international spent nuclear fuel (SNF) transportation*

Munera, H.A., M.B. Canal, & M. Munoz. (1997) 'Risk associated with transportation of spent nuclear fuel under demanding security constraints: The Colombian experience,' Risk Analysis, 17(3), 381-389.

Related factors complicating *safety, security, & safeguards* for SNF in transit:

- Transfers between transportation modes
- Crossing geopolitical and maritime borders



Khlopkov, A. & A. Lutkova. (2010) 'The Bushehr NPP: Why Did It Take So Long?,' Center for Energy and Security Studies, 8.

Introduction (II)

The SNF transportation faces ***more complex risks*** from a growing & evolving operational environment

- Overlaps in risk mitigation responsibilities
- Conflicting objectives
- Increased number of transfers
  - Between transportation modes
  - Across geopolitical/maritime borders

These can directly challenge the ability to maintain ***safety, security, & safeguards*** of SNF

Case Study (I)

Photo of a SNF cask being moved from a container ship to heavy haul truck as part of a multi-modal, multi-jurisdictional international transportation test.
The details are in Paul McConnell et al., 2017. "Rail-Cask Tests: Normal-Conditions of- Transport Tests of Surrogate PWR Fuel Assemblies in an ENSA ENUN 32P Cask".

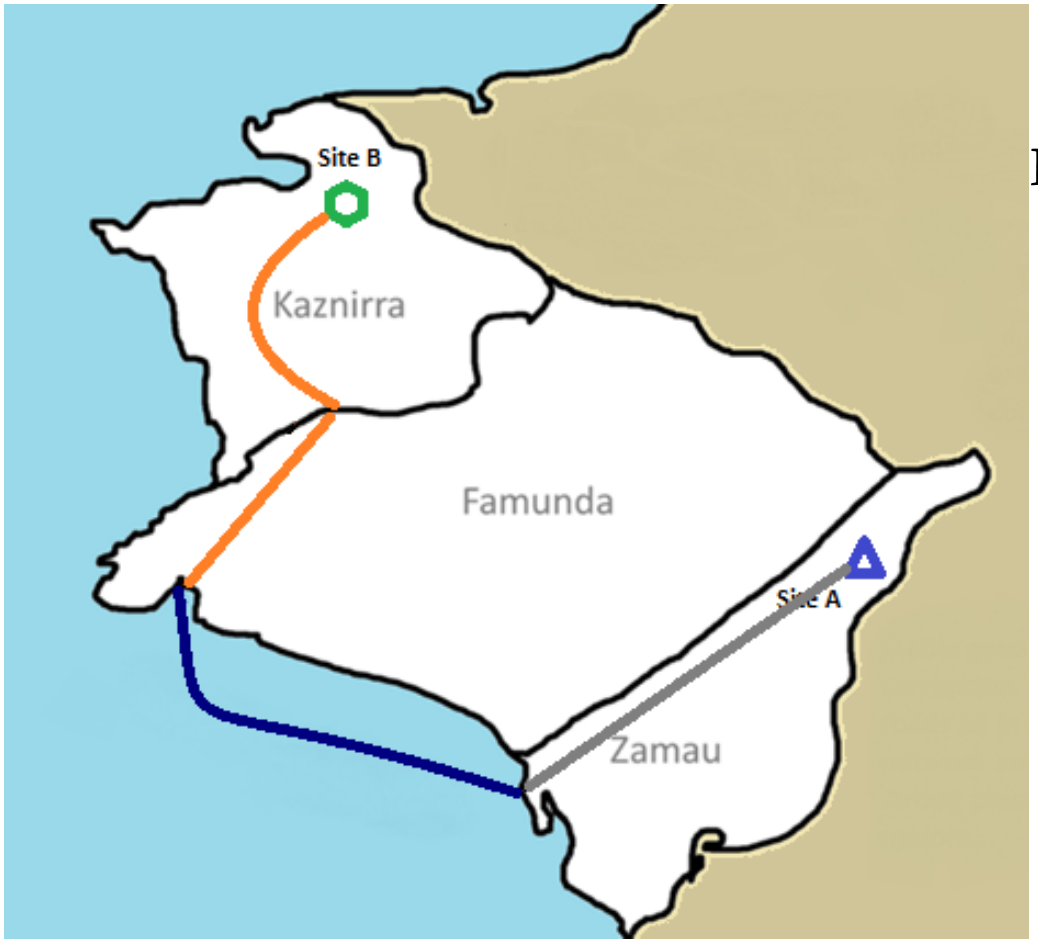
Hypothetical case developed from real-world transportation cases

Details of the case description (& scenarios of concern) briefed to a panel of Sandia SMEs

- SNF transportation operations/safety
- Transportation safety
- International safeguards
- Nuclear security
- Transportation security

No glaring mistakes, omissions or flawed logic were identified

Case Study (II)



ROUTE DESCRIPTION

- SNF cask loaded at the origin facility onto a rail car for transportation to the Port of Zamau (Site A)
- SNF cask transferred from rail car to barge at Port of Zamau (grey line)
- SNF cask travels via international waters to Port of Famunda (blue line)
- SNF is transfer from barge to truck at Port of Famunda
- SNF cask travels by truck to the Famunda/Kaznirra border crossing (Orange line)
- SNF cask arrives for disposition (Site B)

Case Study (III)

Zamau (country of SNF origin)
- Non-weapons state signatory to NPT
- Fairly robust nuclear enterprise (12% of national electrical power)

Famunda (transshipment country)
- Non-weapons state signatory to NPT
- Rampant governmental corruption
- No civilian nuclear infrastructure

Kaznirra (country of SNF destination)
- Non-weapons state signatory to NPT & Additional Protocol
- Well-developed nuclear enterprise

For this presentation, looking at results of:
- Scenario 1: ***Train derailment in Zamau***
  - A 40-foot section of rail track near nuclear power facility is removed
  - The train carrying the SNF cask runs into the missing section of track and derails
  - The damaged cask will be shipped back to Site A & then undergo IAEA inspection

New Analysis Methods: DPRA (I)

Dynamic Probabilistic Risk Assessment (DPRA) analyzes the evolution of various scenario paths between initiating events & possible end states

- A ***bottom-up*** technique that statistically evaluates simulation data from deterministic approaches
- Employs ***dynamic event trees*** for the systematic & automated assessment of possible scenarios arising from uncertainties
- Better accounts for both epistemic & aleatory uncertainties → ***higher fidelity*** analytical conclusions for complex system analysis

DPRA uses ***branching*** & ***editing*** rules to capture basic systems theory concepts for higher fidelity analysis

New Analysis Methods: DPRA (II)

Analysis of Dynamic Accident Progression Trees (ADAPT) software to generate dynamic event trees

- *ADAPT* serves as an overall scenario scheduler to coordinate between three different software codes :
  - RADTRAN (transportation safety)
  - STAGE (security)
  - PRCALC (safeguards)

ADAPT's *branching/editing* rules describe this coordination

New Analysis Methods: DPRA (III)

Branching Condition	RADTRAN Effects	STAGE Effects	PRCALC Effects
Cask Inventory: Burnup, Age	? Alters public consequences of a release	—	? Changes attractiveness of material
Degree of Notice Given to Local Law Enforcement	? Reduces public evacuation time (e.g., release)	? Shortens offsite response arrival time	—

Phased branching conditions & edit rules development:

- **Phase 1**: RADTRAN branching (e.g., between different fuel characteristics)
- **Phase 2**: STAGE branching (e.g., between state or non-state adversaries)
- **Phase 3**: PRCALC branching (e.g., on the amount of fuel dispersed)

➢ RADTRAN, STAGE, and PRCALC can be used to predict more accurate dose and attack difficulties so that we can better predict accurate consequences and responses.

New Analysis Methods: DPRA (IV)

Software Analysis Tool [System Behavior]	Individual Analysis	Integrated Analysis (via ADAPT)
RADTRAN [Safety]	Health effects of radiological release as a deterministic function of the cask inventory	Health effects as a deterministic function of the fuel inventory of the cask influenced by response force ability to prevent sabotage
STAGE [Security]	Security as stochastic parameters of response force & adversary characteristics	Security as stochastic parameters of response force & adversary characteristics conditioned on health effects of radiological release
PRCALC [Safeguards]	Proliferation as function of the total amount of Pu & effectiveness of barriers	Proliferation as a function of the total amount of Pu & effectiveness of barriers conditioned on presence of response forces as a barrier to access

These results illustrate *how DPRA*:

- Uses basic systems theory concepts to ***address system performance*** in complex environments
- Demonstrates it can be extended to ***novel applications***
- Offers additional insights ***to improve*** safety, security, and safeguards as ***desired system-level behaviors***

New Analysis Methods: STPA (I)

Systems-Theoretic Process Analysis (STPA) explores system-level behaviors by looking at how requirements & (un)desired actions interact

- Control actions influence system migration toward/away from ***states of risk*** (that can lead to unacceptable losses)
- A ***top-down*** process that links specific design details to high-level objectives (via hierarchy, emergence, interdependence & feedback)
- Higher levels in the ***hierarchical control structure*** limit how control interactions drive the system into states of higher risk

STPA uses ***control actions*** (& their violations) to capture basic systems theory concepts for higher fidelity analysis

New Analysis Methods: STPA (II)

STPA *abstracts real complex system operations* into

- Hierarchical control structures
- Functional control loops

The underlying logic suggests *redefining the complex risks* associated with the international SNF transportation as

- Identifying requirements
- Enforcing control actions

STPA evaluates the ability to physically move SNF from an origin facility to a destination facility without disruption

- Control actions *describe interactions*

New Analysis Methods: STPA (III)

Increased *hazardous* state [Safety]	Increased *vulnerable* state [Security]	Increased *proliferation* state [Safeguards]	Related Losses
Unplanned radiological release from the cask	Unauthorized access of cask	Loss of 'continuity of knowledge' (material status)	L1, L2, L3, L4, L5, L6
—	Unauthorized access of transportation vehicle	Loss of 'continuity of knowledge' of SNF location	L1, L4, L5, L6

In STPA, the state of increased risk described by "unauthorized access to the SNF" can stem from:

- Intentional use of explosives on the cask
- Unintentional cask breach from derailment

Goal of STPA is to put ***controls*** in place to prevent such states of increased risk

States of increased risk (e.g., hazardous, vulnerable or proliferation states) are ***conceptually equivalent***

New Analysis Methods: STPA (IV)

Control Action	STPA Label: 3S STPA Label	State of Increased Risk (SIR) [STPA hazard type]
Transmit GPS location of SNF cask	SGCA1	SIR10 [$NNP_{1,2}$]
	3SCA1	SIR10, SIR12 [$NNP_{1,2}$]
Stop acceleration once at 55mph	SACA2	SIR4 [NNP_1]
	3SCA4	SIR4 [NNP_1] SIR8 [Too early]
Engage rail car immobilization mechanism	SECA1	SIR5, SIR6 [NNP] SIR5, SIR7 [PNN_1]
	3SCA5	SIR5, SIR6 [NNP] SIR5, SIR7 [PNN_1] SIR2 [PNN_2]

STPA Hazard Types: NNP = "needed, not provided"; PNN = "provided, not needed"; Too early = "provided tool early"
Subscripts denote a particular conditional description for a violated control action aligned with a given state of increased risk

Example: 3S Control action = "physical assessment of cask contents in appropriately sealed facility" (same as Safety CA1)

- As individual safety CA, does not identify related states of increased risk traditionally associated with security:
  - SIR 5 = Unauthorized access of cask
  - SIR 7 = Transportation vehicle stopped longer than expected

These results illustrate *how DPRA*:

- Uses basic systems theory concepts to ***address system performance*** to avoid states of risk
- Demonstrates it can be extended to ***novel applications*** (similarities in states of risk)
- Offers additional insights into how to ***counter threats/ risk from globalized*** environments

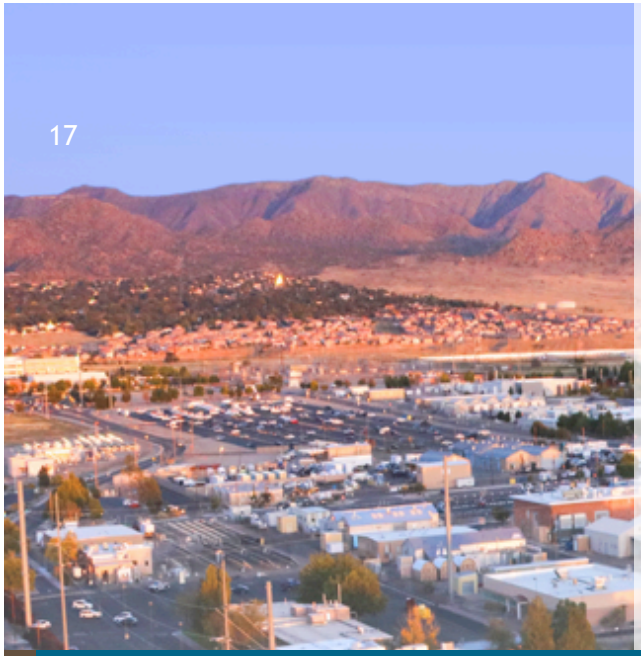
Conclusions

Provided a deeper understanding of ***systemic threats & risks***

- From both ***technical or socio-political*** sources
- Related to safety, security, & safety risks are ***not independent***

Comparing analytical outputs:

- Illustrated how both DPRA and STPA ***included more complexity*** in socio-technical system models to evaluate
- Yielded insights into ***interdependencies & real-world uncertainties into multi-model, multi-jurisdictional*** of SNF transportation
- Indicated that integrated 3S risk assessments ***can be designed to better account for interdependencies*** than independent "S" assessments



QUESTIONS?