This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2018-6984C

Using Systems Theory to Address Complex Challenges to International Spent Nuclear Fuel Transportation

PRESENTED BY

Adam D. Williams

28th Annual INCOSE International Symposium

10 July 2018

SAND2018-???? 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.

Outline

- Introduction
- Basic Concepts in Systems Theory
- New Analysis Methods
  - *Dynamic Probabilistic Risk Assessment (DPRA)*
  - *System Theoretic Process Analysis (STPA)*
- Case Study
  - *International SNF Transportation Hypothetical Case Study*
- Novel Applications
  - *Analytical Results*
- 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

Introduction (III)

According to a former Deputy Director-General of the International Atomic Energy Agency:

- "***Safeguards, security, and safety*** are commonly seen as ***separate areas*** in nuclear governance. While there are technical and legal reasons to justify this, they also ***co-exist and are mutually reinforcing***. Each has a ***synergetic effect on the other***, and authorities should carve out avenues for collaboration to contribute to the effectiveness of the nuclear order."

Traditional risk analysis methods ***struggle*** to account for these "synergistic effects"

- Recent Sandia National Laboratories study argued that ***applying basic systems theory*** concepts ***can address*** these challenges

Basic Concepts in Systems Theory

International SNF transportation can be described in terms of

- ***Organized complexity*** (e.g., "many, but not infinite" # of components)
- ***Dynamics*** (e.g. ordered systems migrate toward greater disorder)
- ***Interdependence*** (e.g., interactions affect behaviors)
- ***Hierarchy*** (e.g., relationships between levels of complexity)
- ***Emergence*** (e.g., irreducibility of certain system behaviors)

These ***concepts help describe these challenges*** to SNF transportation

Safety, security, & safeguards of SNF → ***emergent system properties***

New Analysis Methods: DPRA

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: STPA

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

Case Study (I)

Photo of a mock SNF cask being moved from a container ship to heavy haul truck as part of a multi-modal, multi-jurisdictional international transportation route. Copyright: Sandia National Laboratories.

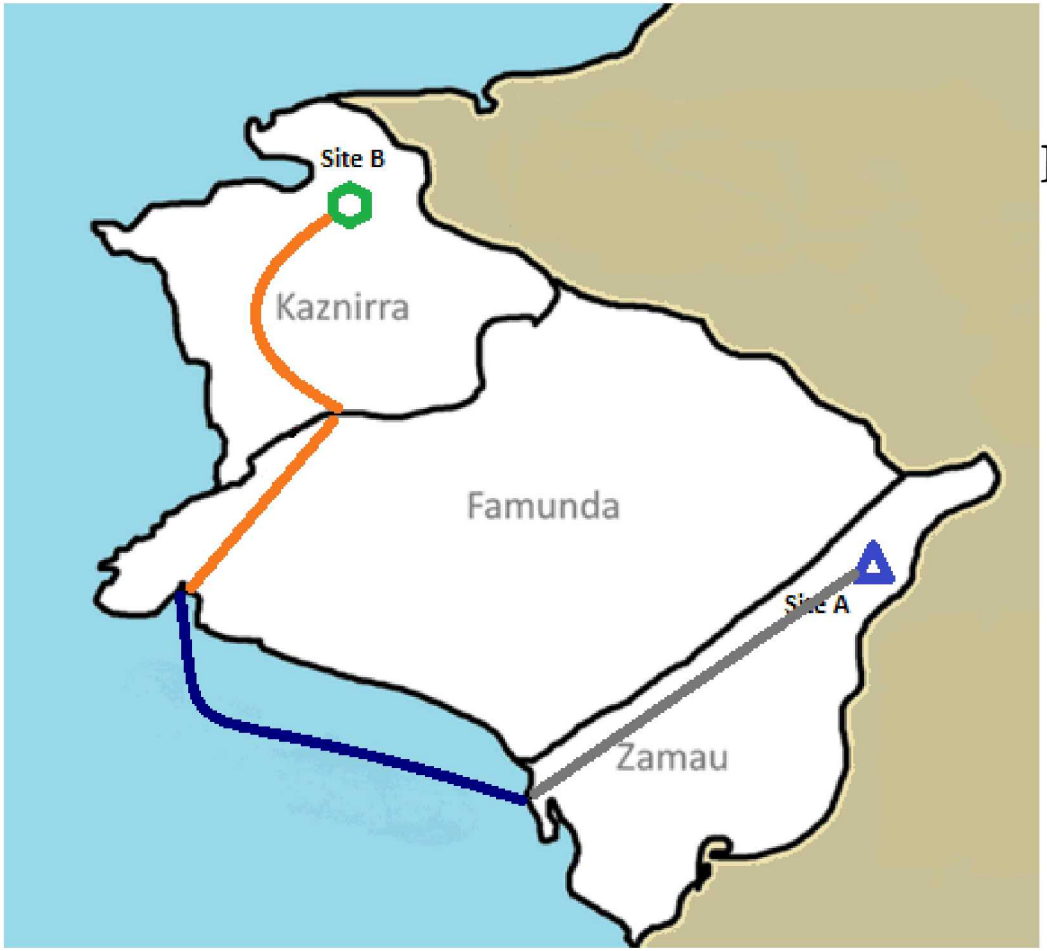
Hypothetical case developed from real-world transportation cases

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 the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) with a fairly robust nuclear enterprise provides 12% of national electrical power

Famunda (transshipment country)

- Non-weapons state signatory to the NPT with rampant governmental corruption and no civilian nuclear infrastructure (SNF transit country)

Kaznirra (country of SNF destination)

- Non-weapons state signatory to the NPT & Additional Protocol with a well-developed nuclear enterprise interested in making Site B a regional SNF repository

For this presentation, looking at results of:

- Scenario 1: ***Train derailment in Zamau***
- A 40-foot section of rail track on the outskirts of the city that hosts the Zamaun nuclear power facility is removed. The train carrying the recently-loaded SNF cask to the Port of Zamau runs into the missing section of track and derails.

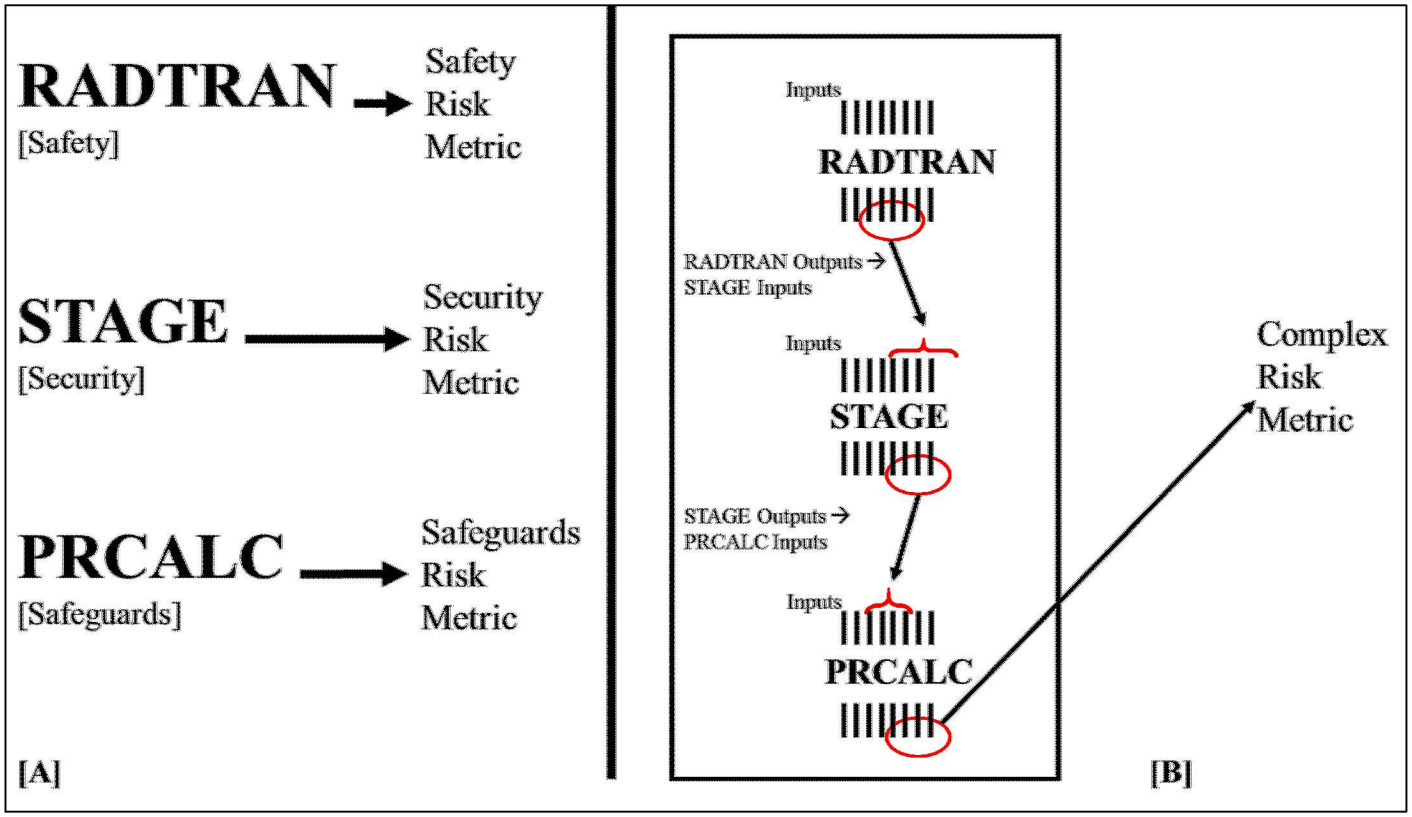
Novel Applications: DPRA (I)

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

Novel Applications: DPRA (II)



GOAL:

outputs of traditionally isolated 'S' codes

vs.

outputs coordinated through ADAPT

Novel Applications: 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)

Interdependence → deterministic health effects vs. sabotage

Hierarchy → security escorts help constrain safeguards violations

Emergence → deleterious effect of the release on security force

Novel Applications: 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***

Novel Applications: STPA (I)

STPA ***abstracts real complex system operations*** into

- Hierarchical control structures
- Functional control loops

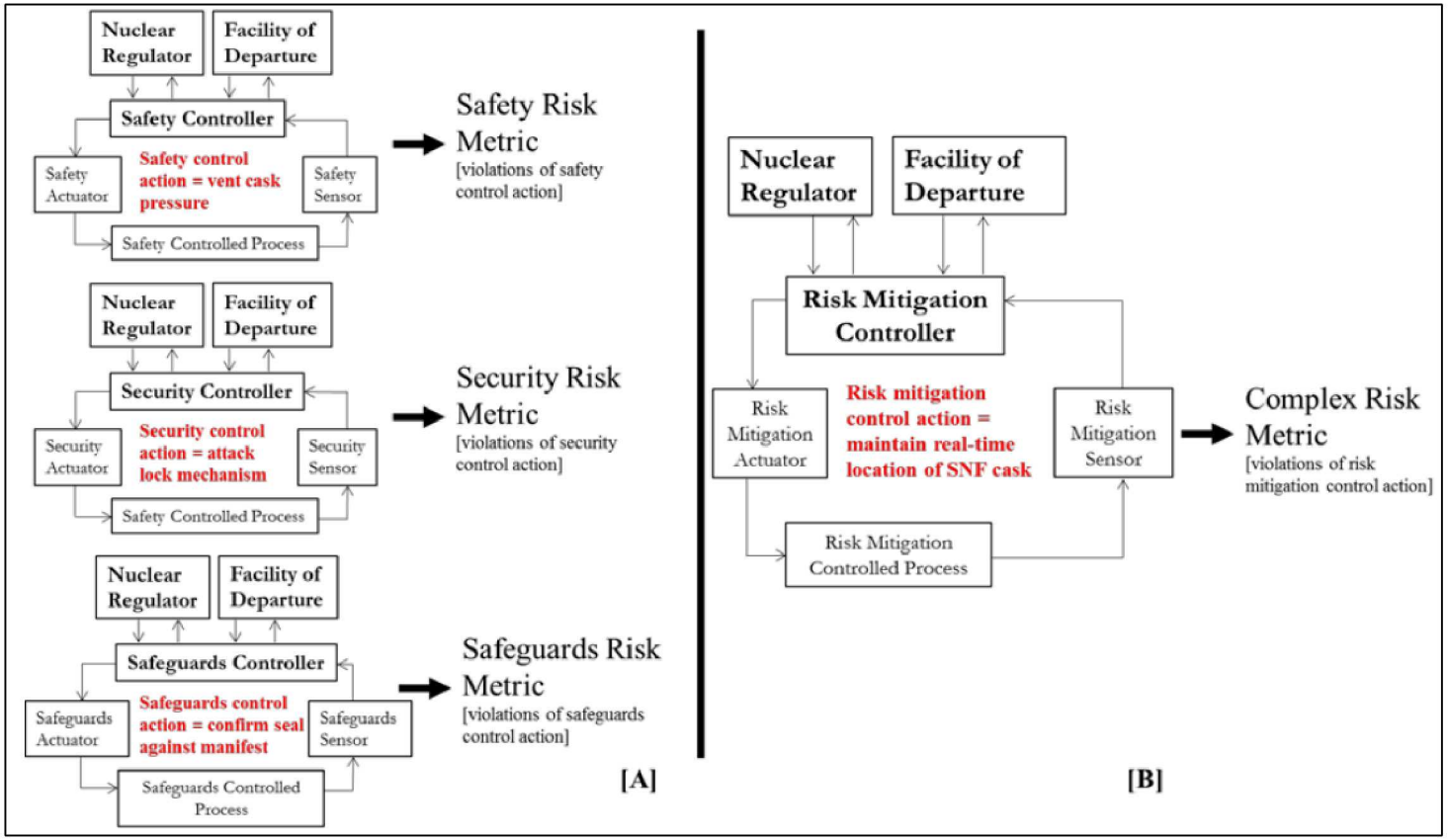
The underlying logic suggests ***redefining the complex risks*** associated with the international SNF transportation as

- 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***

Novel Applications: STPA (II)



GOAL:

outputs isolated 'S' STPA

vs.

output of a 3S HCS STPA

Novel Applications: 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***

Novel Applications: 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

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 (I)

Results of both DPRA & STPA demonstrate ***utility of basic systems theory concepts*** for complex risks

Designing/operating systems to ***leverage interdependence & hierarchy*** to constrain behaviors of lower levels can guide emergent behaviors

Basic ***system theory concepts better align*** with operational uncertainties & multi-level interactions of ***multi-model, multi-jurisdictional*** systems

Conclusions (II)

Basic systems theory concepts to evaluate international SNF transportation identified:

- ***Gaps*** (e.g., the potential for there to be no shipment oversight entity),
- ***Interdependencies*** (e.g., coordinate security and emergency after train derailment)
- ***Conflicts*** (e.g., inspectors may have both safety and safeguards responsibilities)
- ***Leverage points*** (e.g., security procedures to maintain "continuity of knowledge")

Insights indicate that integrated 3S risk mitigation strategies can be designed ***to better account for interdependencies*** not included in independent "S" assessments

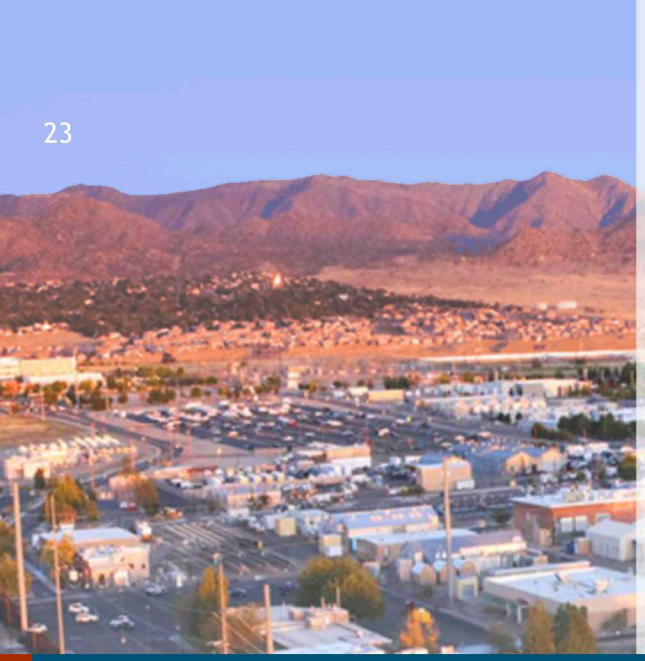
Conclusions (III)

Results are compelling, but limitations exist:

- Inability to directly link insights to real-world occurrences limits the
- The complication of linking software codes prevented establishing "clean" linkages

Yet, insights useful for enhancing other complex systems research at Sandia:

- Investigating expansions to PRA for safety & security in the NFC (Forrest *et al.* 2017)
- Providing a more holistic approach to the socio-technical nuclear landscape (Bonin *et al.* 2017)
- Overcoming gaps in addressing risk complexity in the NFC (Williams & DeMenno 2017).



QUESTIONS?