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.

SAND2019-9008C

Advancement of Dynamic Assessment Methodologies for Transportation Security

PRESENTED BY

Adam D. Williams, Doug Osborn, & Brian Cohn

International Symposium on the Packaging and Transportation of Radioactive Materials

4-9 August 2019

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.

SAND2019-XXXX 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.

Introduction

Global interest in expansion of nuclear fuel cycle (NFC) activities driven by:

- Increasing energy demands (e.g., electricity generation and water desalination)
- Calls for "carbon-free" energy programs
- Development of small modular reactors with reduced capital outlays

Increases to NFC activities expands the extent and form of transportation of spent nuclear fuel (SNF)

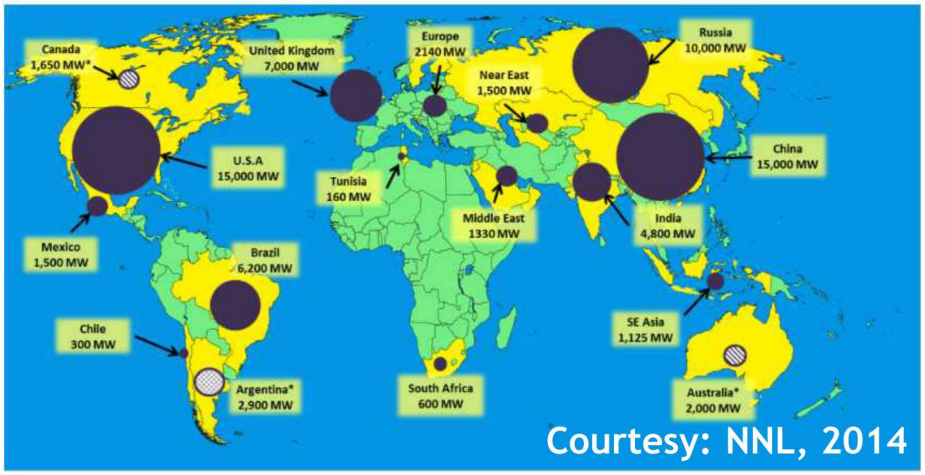


Photo of a mock SNF cask being moved from a container ship to heavy haul truck as part of a multi-modal, multi-jurisdictional international transportation route. Copyright: Sandia National Laboratories.

Introduction

Safety, security & safeguards (3S) ***complexity*** threatens to ***challenge*** the scope of current analysis

Interactions between different 3S elements as ***important & influential*** as individual analyses

Dynamic methodologies created an integrated approach to investigate 3S behaviors, including interactions

- Dynamic Probabilistic Risk Assessment (DPRA)
- System Theoretic Process Analysis (STPA)

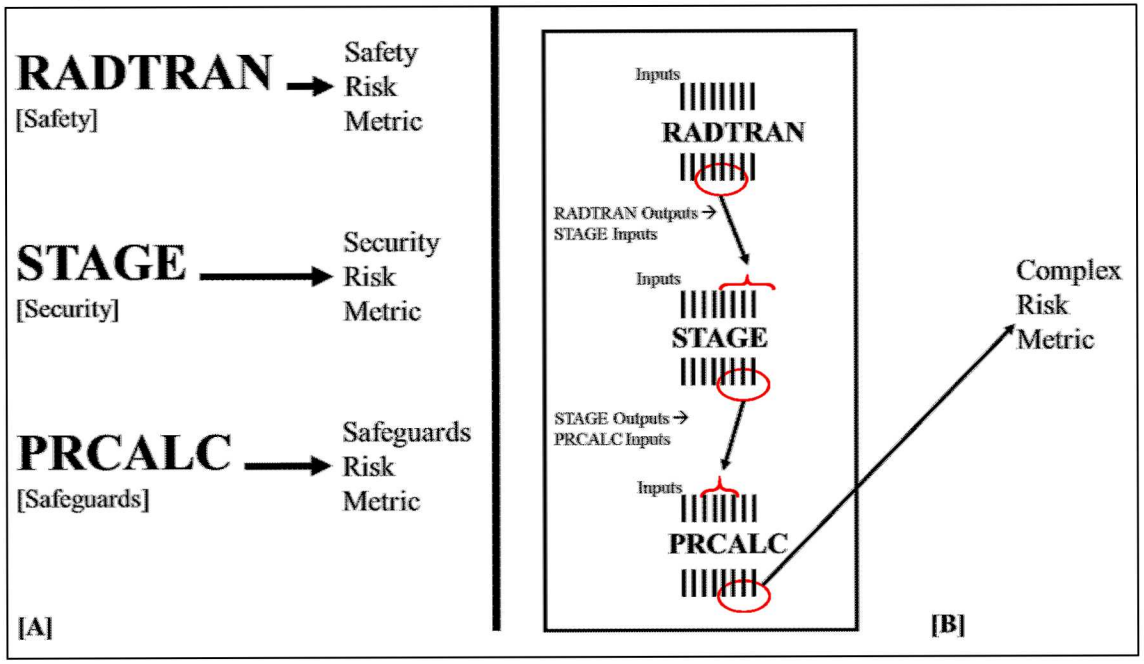
DPRA Overview

DPRA

- "Bottom up" approach
- Deterministic models of system states that evolve through time

Dynamic Event Trees (DETs)

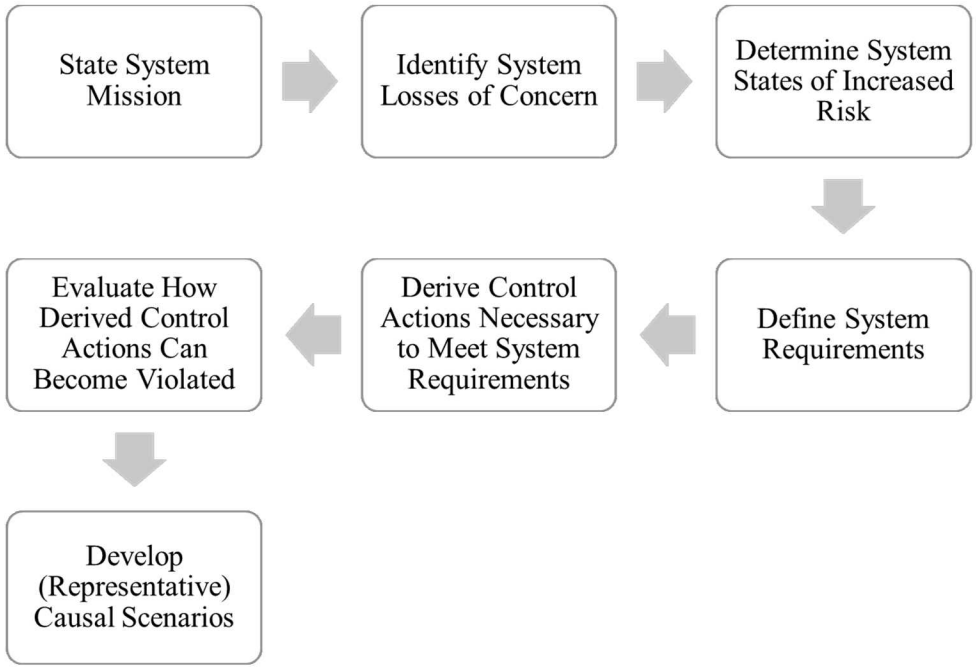
- Similar to traditional PRA
- System begins in one state and branches at points of uncertainty



STPA Overview

STPA
- "Top down" approach
- Hierarchical control structures to model emergent system properties

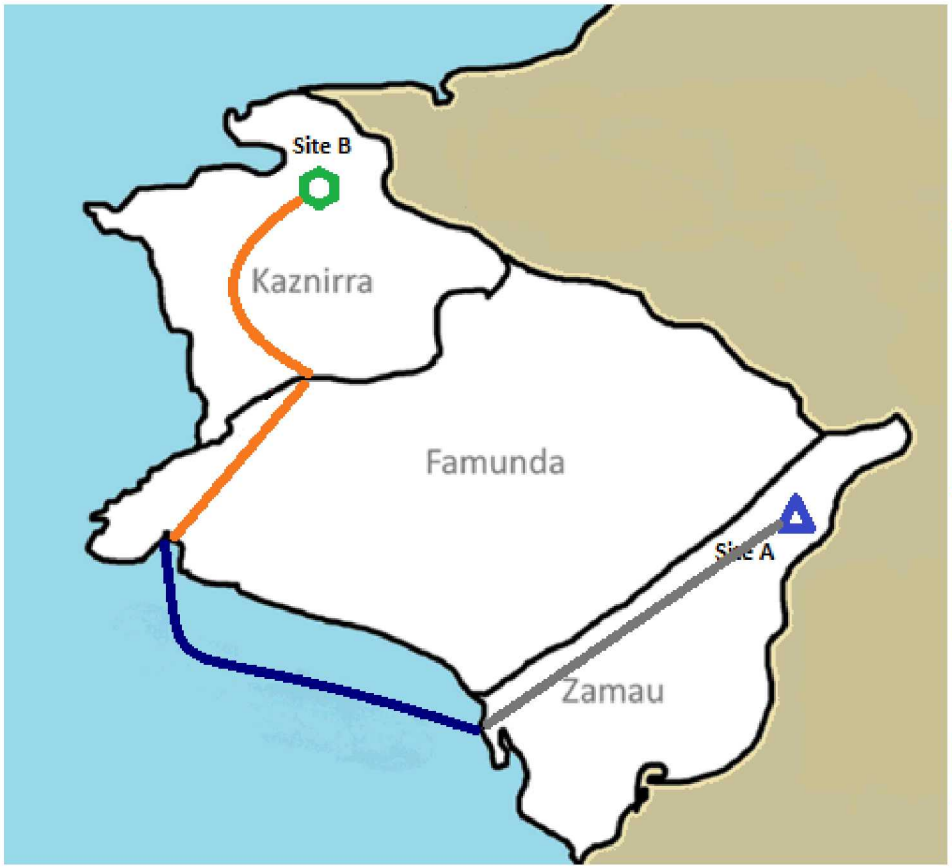
Hazardous system states are
- Logically categorized to determine the failures in control actions
- Undesired control actions → states of higher risk



Case Study

A hypothetical set of countries and SNF route was developed, including:

- Zamau (e.g., origin facility)
  - From here, SNF is transported by rail
  - Loaded on barge at the Port of Zamau
- Famunda (transshipment country)
  - SNF is offloaded at the Port of Famunda
  - SNF is transported by road to Kaznirra
- Kaznirra (e.g., SNF repository site)
  - SNF transported by major highway



Case Study

A scenario* was created to evaluate the 3S methodologies

- During transit through Zamau, a 40 foot section of track is missing
- The train derails upon reaching the missing track
- A state actor posing as terrorists attack the derailed train
- Upon success, attackers divert one significant quantity of Pu
- Missing fuel is replaced with dummy fuel and detonated with TNT
- Cask remains are returned to Site A and IAEA is notified

The scenario highlights 3S interactions and does not fall cleanly within one element

*This scenario was vetted but a multidiscipline group of Sandia SMEs…

DPRA Methodology

Three codes are used for the 3S analysis

- RADTRAN: Safety
- STAGE: Security
- PRCALC: Safeguards
- Driven with ADAPT

Branching rules were constructed to model scenario uncertainties:

- Cask Inventory
- Advanced Local Law Enforcement (LLE) Notification
- Early Discovery of Track Damage
- Severity of Derailment
- Size of Attack

DPRA Results

DPRA couples safety, safeguards and security through branching conditions

- One branching condition can have ***conflicting individual outcomes***

Each branching condition can be investigated individually

- LLE notification reduces evacuation times
- Reduces offsite LLE response for security events
- May be leaked to attacking groups

		Output Measure	
		Maximum Individual Dose (rem)	Average P_N
Scenario	Full Scenario	82.09	65.91%
	Advanced LLE Notice	81.36	72.38%
	Minimal LLE Notice	82.82	59.46%

STPA Methodology

STPA identifies hazardous states that impact 3S

Defines requirements to prevent the hazardous state

Translates requirements into control actions per system actor

Emergent Property	State of Increased Risk	System Requirement	Representative Control Action [Specific Controller]
Security	Unauthorized access of cask*	Unauthorized individuals must not access the 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 Security Authority]

Integrated 3S Analytical Results

Using STPA, violated control actions in one domain (e.g., security) can produce undesired states of increased risk in another (e.g., safety or safeguards)

- Traceability between control action violations & states of increased risk

For example, if the high-level security requirement "prevent unauthorized access to the cask" is violated:

- Could result in an unplanned radiological release (a safety hazard)
- Could cause loss of continuity of knowledge (a safeguards issue)

Therefore, ***interdependencies*** can be exploited to enhance operational efficiency or reduce costs/risks

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

Implications for Combined Analysis

STPA's strengths are in systematic generation of scenarios
- Weakness is an inability to prioritize the set of hazards

DPRA's strengths are in quantitatively exploring scenarios
- Provides little information on generation of scenarios

A combined approach may combine the benefits of both
- STPA generates scenarios
- DPRA executes scenarios

Conclusions

Trends in SNF transportation suggest more complex NFC activities

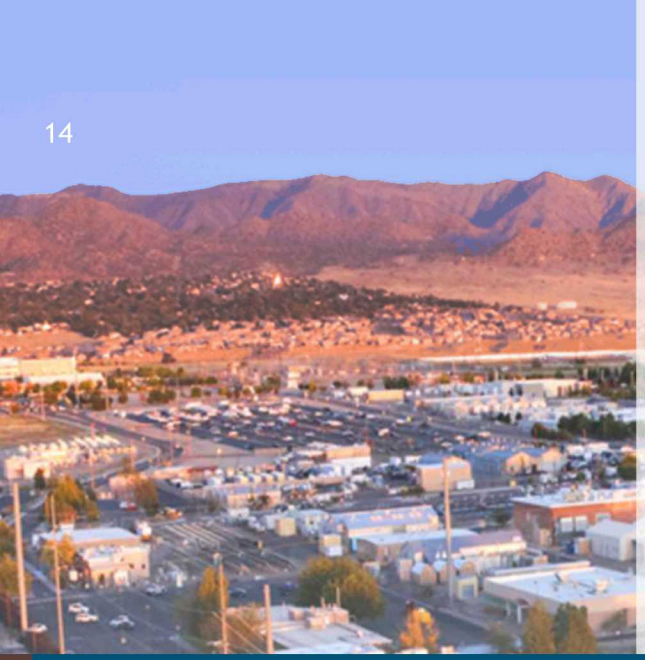
- Smaller entities shipping nuclear materials
- More international transportation of nuclear materials

Integration of safety, security and safeguards into 3S analysis

- Is necessary to ***model interrelations***
- May improve efforts to ***reduce risk*** and ***improve performance***

DPRA and STPA have demonstrated capability to integrate safety with security

- Sandia is currently pursuing additional R&D to both further exploit this interaction & incorporate international safeguards for global NFC activities



QUESTIONS?