Exceptional service in the national interest

Sandia National Laboratories

Capturing Human, Social & Organizational Influences on Nuclear Security:

System-Theoretic Assumption Guided Evaluation (STAGE)

Adam D. Williams

Sandia National Laboratories is a multi-program laboratory managed and 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. SAND NO. 2017-XXXXP

Outline

- Introduction
- STAGE: System Theoretic Assumption Guided Evaluation
- Analysis & Discussion
- Summary & Conclusions

DISCLAIMER
The views expressed in this document are related to my doctoral research at MIT's Engineering System Division. In addition, they are solely those of the author and do not reflect the official position of policies of Sandia National Laboratories, the Lockheed Martin Corporation, the National Nuclear Security Administration, the Department of Energy or the United States Government

Introduction

- Per WINS: ‘An organization may be ***technically competent*** while ***remaining vulnerable*** if it discounts the role of the human factor’ (2016)
  - Address General Eugene Habiger – ‘Good security is 20 percent equipment and 80 percent culture’

- Traditional security analysis approaches emphasize technological solutions to minimizing challenges to probabilistic measures of security effectiveness
  - But, risk-based approaches ‘cannot address cultural or organizational barriers to improved security’ (NAS 2010)

- In response, recent trends have emphasized security culture & governance to address the ‘human’ factor on security performance
  - ‘While the IAEA has released methodologies on evaluating vulnerabilities and physical protection, it has not yet introduced guidelines on assessing the human factor in detection, delay, and response’ (Khripunov 2014)

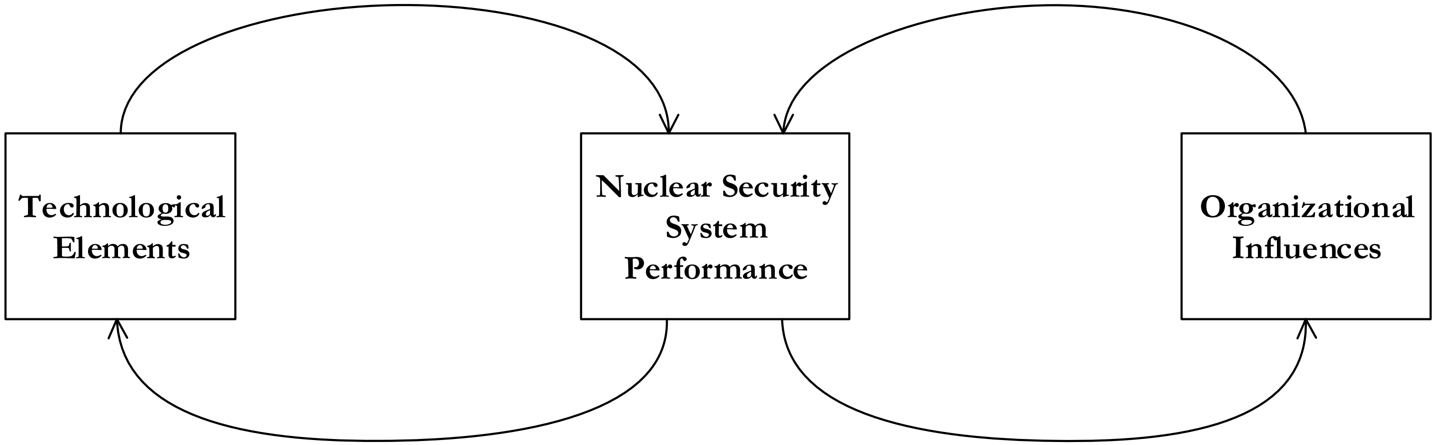
Introduction

- Per one U.S. nuclear security expert:
  - 'Culture does not exist in a static environment, and there are pressures, both positive and negative, at all times. Organizations…need to…control and influence the factors that create a culture enabling mission success everyday' (NAS 2015)

- **GOAL**: is to provide an analytical process to address this gap by evaluating how organizational influences support or undermine design assumptions
  - Go beyond improvements in nuclear security culture
  - Tie the 'human factor' to risk-based security system performance metrics (detect, delay & response) via design assumptions

STAGE

- System-Theoretic Assumption Guided Evaluation (STAGE), argues that
  - Security system performance emerges from interactions of social/organizational and technical components


Technological Elements
Nuclear Security System Performance
Organizational Influences

  - Security system performance must consider how closely the actual & expected operational environments align
    - The larger the difference between expected & experienced operational environments, the less able the security system is to achieve desired performance metrics

STAGE

- Organization science suggests that the organization can pay a key role in **reinforcing** or **opposing** the alignment of actual & expected operational environments

- STAGE argues that 'operational environment' can be described in terms of ***organizational influences*** that
  - Must be provided to support the completion of desired security tasks
  - Are observable/controllable by the organization

- Expectations about organizational influences by security designers can be described in terms of ***assumption categories***
  - Help to determine organizational influences necessary for nuclear facilities to provide in order to align operational realities with the expected operational environment (undergirding security system design)

STAGE

- Defining the operational environment the organizational influences that ***must be provided*** to support the completion of security-related work tasks to ***reach desired performance goals***
  - Identifies the causal relationships between related organizational influences & technological elements that effect security performance
  - Builds on nuclear security culture & governance that offer lists of organizational influences identified by a range of nuclear security professionals, practitioners & experts

- STAGE, then,
  - Represents a logical path between nuclear security culture (e.g., organizational influences) & risk-based analyses (e.g., security system performance)
  - Offers an analytical capability to assess how organizational influences may violate security system performance expectations
  - Identifies how to move the actual operating environment closer to the expected operational environment to better approach expected system performance

Analysis & Discussion

- Consider a hypothetical case of international transportation of spent nuclear fuel (SNF) from Country A to Country C
  - Country A (stable government & strong transportation infrastructure)
    - Generates the SNF
    - Hosts a port capable of loading/unloading SNF shipments via barge
  - Country B (quasi-stable government & weak transportation infrastructure)
    - Geographically located between Country A & Country C
    - Hosts a port capable of loading/unloading SNF shipments via barge
  - Country C (stable government & strong transportation infrastructure)
    - Hosts SNF disposal site
    - Does not host a port capable of loading/unloading SNF shipments via barge

Analysis & Discussion

- Goal is for SNF travel from Country A to Country C via:
  - SNF cask is loaded in Country A onto a rail car for transporation to the Port of Country A where it is loaded onto a barge;
  - SNF cask travels via international waters to the Port of Country B in the northwest corner of the country and loaded onto a truck; and,
  - SNF cask travels by road through western Country B, across the border and across interior Country C to the disposal site

- To focus analysis, consider the following scenario:
  - Transfer of security responsibility from Country B officials to Country C officials as the SNF crosses the border
    - Highlights insights provided in WINS/WNTI best practices documentation

Analysis & Discussion

- One desired security performance metric is **increased delay** via
  - Locking tie-down mechanisms to secure the cask to the transportation vehicle
  - Which is only achieved when the related work task of attaching (or verifying the attachment of) the locking tie-down mechanisms to the transportation vehicle is completed

- Further, STAGE identifies the following capabilities necessary for an individual to complete this security-related task:
  - The required level of knowledge is defined & communicated
  - The required resources are known & provided
  - Workforce norms support task completion
  - That users & management have an aligned level of knowledge of system performance

- These capabilities determine the necessary organizational influences to ensure the desired increase in delay

Analysis & Discussion

- STAGE also helps identify who and/or how the organizational influences are provided
  - E.g., the same technology (e.g., locking tie-down mechanism) employed in different operational environments requires the **same capabilities** for task completion, but likely through **different organizational influences**

- Example: organizational influences to support locking tie-down task completion in
  - Countries A & C provided by robust competent security authority
  - Country B provided by entity with part-time nuclear security responsibility or may not be provided at all

- STAGE identifies
  - Potential, non-traditional challenges to security effectiveness
  - Specific area(s) for security system performance improvement

Summary & Conclusions

- Summary
  - Security designers make assumptions about the operating environment for security systems—suggesting any divergence by actual operations may cause degraded system performance
  - Organizational threats to security performance can be expressed in terms of influences on capabilities required for security task completion
    - Providing additional avenues for improving security system performance
  - STAGE offers a method for identifying organizational influences that underlay security system assumptions to improve the security of nuclear materials
    - Fills a gap between the technical focus of traditional nuclear security analysis (e.g., DEPO) & the recent emphasis on nuclear security culture and governance

Summary & Conclusions

	DEPO (ITC)	IAEA Nuclear Security Culture	WINS Nuclear Security Governance	STAGE
Definition of security	Probabilistic ability of PPS components to detect, delay and respond to adversaries along predetermined paths	Prevention, detection & response to, malicious acts (theft, sabotage) involving nuclear/ radioactive materials or facilities	Governing the effective application of security measures to mitigate threats within the operational environment	Emergent property of interacting organizational & technical components within a 'systems' perspective of a nuclear facility
Treatment of Organizational Factors	As one time probabilities of human error	As factors for self-assessment in the IAEA nuclear security culture model	In terms of hierarchical management structures and responsibilities	As controllable, dynamic influences on user capability to complete work tasks undergirding security system design
Security Improvements are	Technical 'add-ons' to already operating nuclear facility security systems	Tangible & intangible actions taken to reinforce that a credible threat exists & that security is important	Based on inter-related voluntary/ regulated policies, procedures & decisions	Both technical & organizational influences enabling completion of work tasks to meet desired security performance