SAND2017-11979C

A System-Theoretic Approach to Overcoming Cultural & Organizational Barriers to Nuclear Security Improvement

Adam D. Williams

Global Security Research & Analysis

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and 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-NA-0003525. SAND2017-XXXX

Outline

- Introduction
- Addressing Cultural & Organizational Barriers to Security Performance
- A New Approach for Cultural & Organizational Barriers
- Lessons from International Spent Nuclear Fuel Transportation
- Summary & Conclusions

DISCLAIMER

The views expressed in this document are SOLELY THOSE OF THE AUTHOR & 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 National Technology & Engineering Solutions of Sandia, Honeywell International , the National Nuclear Security Administration, the Department of Energy or the United States Government

Introduction

- In the words of others:
  - 'An organization may be ***technically competent*** while ***remaining vulnerable*** if it discounts the role of the human factor' (WINS, 2016)
  - Risk-based approaches to nuclear security 'cannot address ***cultural or organizational barriers*** to improved security' (NAS 2010)
  - '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)
- These quotes suggests a need to better incorporate the ***interaction(s)*** between ***technical & social components*** into nuclear security analysis

Addressing Cultural & Organizational Barriers

Sandia National Laboratories

- Traditional approaches to nuclear security analysis:
  - Make assumptions about how the PPS will be used in operation that ignore organizational context
  - Can be challenged by geopolitical disputes, bureaucratic processes, reliance on secrecy
  - Focus on designing to the facility mission (e.g., often profitability) which commonly assumes that current security protocols are 'good enough'
- Yet, there is still the ***EXPECTATION*** for high levels of security personnel vigilance to meet PPS performance goals

Addressing Cultural & Organizational Barriers

- Recent approaches to address cultural & organizational barriers to security performance are exemplified in the IAEA's Nuclear Security Culture Model
  - Built on Schein's theoretical model of organizational culture
    - Basic assumptions→Espoused values→Artefacts
  - Offers descriptive characteristics of
    - Individual (leadership [8] & personnel [5]) behaviors to 'foster more effective nuclear security'
    - Management systems (17) that 'prioritize security'
- Seems to assume that once these characteristics are established, they will be steady over time

Addressing Cultural & Organizational Barriers

Sandia National Laboratories

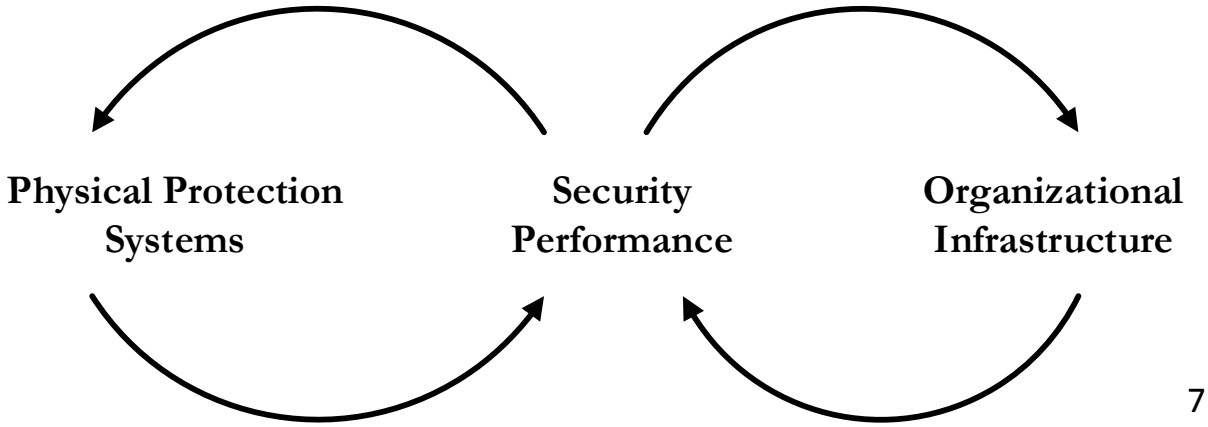
- Though a widely used & useful framework for addressing some of these barriers, this underlying assumption struggles to account for how
  - Challenges to securing nuclear materials and facilities are
    - Varied (e.g., outside, insider, cyber)
    - Ever present (e.g., rise of new terrorist or criminal groups)
    - Do not only stem from adversary action (e.g., performance can be diminished without presence of an adversary)
  - Human & organizational influences (& their interactions) impact security often acting as barriers to desired performance levels

A New Approach

- Based on evaluating how system-level interactions between ***PPS*** & ***organizational infrastructure influences***

- Incorporates tenets of systems theory & organization science
  - Human behavior is required to enact the PPS to achieve desired performance
  - The PPS is necessary to guide human behavior to achieve desired performance

- Argues that security performance ***emerges*** from interactions among ***PPS components*** & ***human behaviors*** within organizational infrastructures



A New Approach

- Therefore, security performance can be described in terms of how these interactions accomplish high-level ***detection, delay*** & ***response*** security functions
  - These functions are often captured in security performance specifications
- Yet, there are a few ***key assumptions*** underlying performance specifications
  - (1) the required task is identified & assigned
  - (2) the standard for task completion is met
  - (3) completion of the required task supports high level security functions
- Here, desired levels of security performance require ***BOTH***
  - An adequately designed PPS be able to achieve the performance specifications
  - The validation of these 3 assumptions on PPS use

A New Approach

- As such, this approach argues that to achieve desired levels of security performance
  - The PPS is necessary to guide human behaviour, ***AND***
  - Human behaviour (assumptions on PPS use) is required to enact the PPS

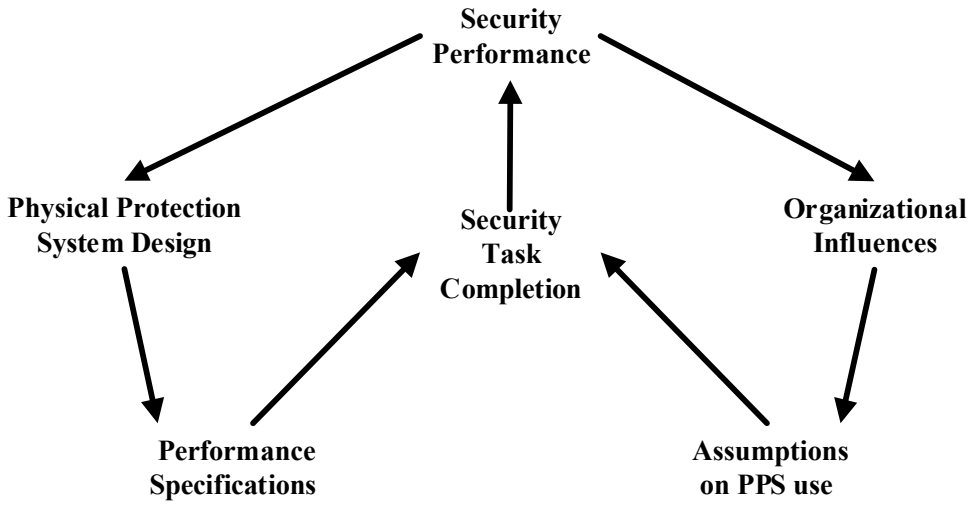
- Desired security performance, then, occurs when
  - Security task completion accomplishes security functions
  - Performance specifications align with assumptions on PPS use ***AND***
  - Organizational influences support the validity of these assumptions

- Organizational influences can ***support*** or ***oppose*** these assumptions on PPS use

A New Approach

- Assuming a fully functional PPS with clear performance specifications, a ***security task completion approach*** provides
  - An explanation for how non-technical influences can cause sub-optimal security performance
  - A mechanism for addressing the gap between the IAEA nuclear security culture model & detection, delay & response performance measures

- The analytical focus ***shifts*** from identifying individual behaviours to assessing how organizational influences impact assumptions on PPS use



Lessons from SNF Transportation

- 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

- The ***security task completion approach*** provides a rigorous, objective method for evaluating (potential) incongruities in security performance
  - By related various entities
  - Along an international transportation route

Lessons from SNF Transportation

- This ***security task completion approach*** explicitly includes operational context as a causal factor in security performance
  - A potential improvement over traditional approaches that struggle to account for the expanding complexities of securing SNF during global transit

SNF Transportation Security Implementation Decision *(related security task)*	**Organizational Influences[a]**	**Impact on Assumptions on PPS Use**	**Effect on Security Performance[b]**
Not agreeing on clear security responsibility transition protocols at a land border crossing *(assess/reconcile intrusion detection sensor)*	• Unclearly communicated security expectations • Lack of feedback channels	• The required task(s) not identified & assigned • The standard for task completion cannot be met	Detection-related security tasks not completed → decreased P_D → decreased security performance

[a]Described in terms of those offered in Williams (2017)

[b]In terms of traditional security performance measures: probability of detection (P_D), delay time (t_D) & response force time (RFT)

Lessons from SNF Transportation

Sandia National Laboratories

- Cultural & organizational barriers can materialize into increasingly complex risks against achieving desired levels of security performance

- The ***security task completion approach*** offers one option for identifying organizational influences to help overcome these risks

- For SNF transportation, specifically, the ***security task completion approach*** better addresses the challenges of this transborder, multi-modal distributed process
  - Can help design more robust PPS
  - Can identify misalignment in organizational influences on security

Conclusions

- The ***security task completion approach*** argues that interactions between social & technological components better explains 'non-traditional' challenges to security performance
  - E.g., the security impact of an increasing number of SNF cask transfers between transportation modes (e.g., road to rail to water)

- Forthcoming research results introduce how this **security task completion approach** is incorporated into a system-theoretic analysis framework
  - Which offers potential benefits for PPS designers, security operations assessors (or managers) & security performance oversight entities

- Overall, the ***security task completion approach*** shows promise for overcoming cultural & organizational barriers to improving performance in our increasingly dynamic security environment