SAND2018-7206C

New Thoughts on Protecting Nuclear Materials & Facilities: A Systems-Theoretic Framework for Security

PRESENTED BY

Adam D. Williams

59th Annual Meeting of the Institute for Nuclear Materials Management

22-26 July 2018

SAND2018-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.

Outline

- Introduction
- Challenges to Security at Nuclear Facilities
- Including Human/Organizational Behaviors in Nuclear Security
- A New Approach: The Systems-Theoretic Framework for Security (STFS)
- Contributions of the STFS to Improving Nuclear Security

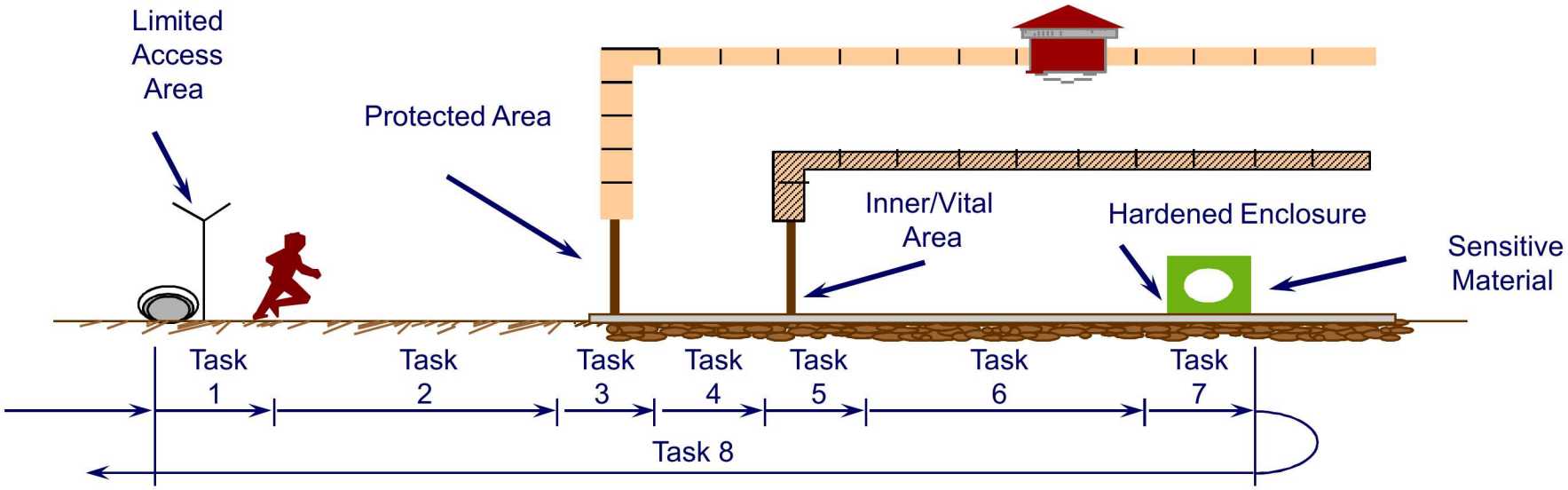
Introduction

According to a former nuclear security manager: During a physical protection system (PPS) upgrade closeout visit to a Russian nuclear facility in the 1990s

- Upon arriving, U.S. team informed the inspection date fell on a newly established national holiday & informed that no one would able to host them at the facility
- The team did not consider this a problem, they ***assumed*** that security personnel would be on site to protect the special nuclear material (SNM)
- Arriving at the site, neither guards nor central alarm station (CAS) operators present, and the PPS was turned off
- The team learned the PPS was ***always turned off on weekends and holidays*** to locally-mandated meet power use limits
- It seemed that the facility felt this was acceptable security behavior—ultimately putting the SNM at risk in order to meet an electricity use quota

Despite having the ***right technology*** in place, the interaction of technology with human operators resulted in reduced security at this facility.

Challenges to Nuclear Security (1/2)



Security of nuclear facilities and materials faces many challenges

- Multiple types of malicious acts [Bunn 2009]
- Cyber-based intrusions [EPRI 2015]
- Insider threat [Bunn & Saga 2014]
- Social engineering of personnel [Abraham & Chengalur-Smith 2010]
- Unmanned aerial vehicles [Solodov, Williams, Al-Hanaei & Goddard 2017]
- Internal politics & bureaucratic inertia [Nuclear Threat Initiative 2016]

Challenges to Nuclear Security (2/2)

According to Dr. Igor Khripunov, nuclear security culture expert:

> "While the International Atomic Energy Agency [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*** the three main pillars of security"[Khripunov 2014, p. 39-40]

A common understanding is echoed by former Department of Energy security czar Gen. Eugene Habiger:

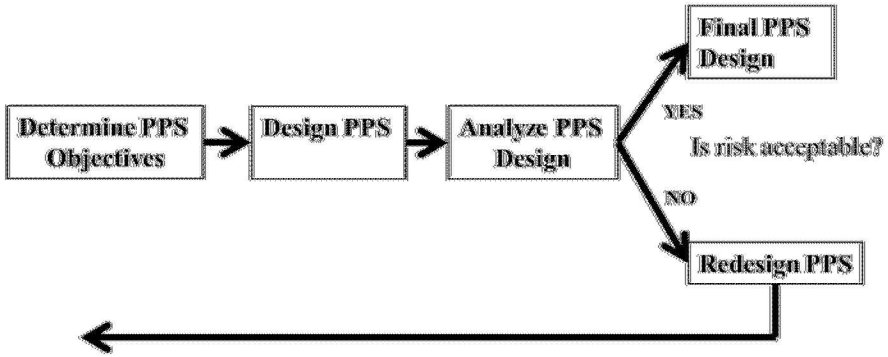
> "good security is 20 percent equipment and 80 percent culture" [Bunn & Sagan 2014, p. 10]

No one has yet figured out a way to understand how human & organizational factors might influence PPS effectiveness

Including Human/Organizational Behaviors (1/2)

Technology-Based Approaches

Emphasizing technology-centric solutions to minimize vulnerabilities from changing adversary capabilities



Implicitly assumes tasks will be completed ***adequately*** & with ***high quality***

Human-Based Approaches

Balance importance of protecting nuclear materials with "boredom" of securing them [Charlton & Hertz 1989]

Indicates importance of ***non-technical influences*** on security performance

Including Human/Organizational Behaviors (2/2)

Neither of these current approaches account for ***socio-technical interactions***

Ignoring these interactions ***limits*** security assessment to reconcile ***daily security performance*** with ***operational requirements***

Human/organizational behaviors are significant influences

- "every dollar that a facility spends on protection is a dollar *not* spent on revenue-generating production" [Bunn 2005]

There is still a need to better understand the relationship between:

- Human/organizational behaviors
- PPS technology
- Security performance

A New Approach: STFS (1/4)

Primary argument: security performance affected by ***both***

- Technical (e.g., PPS)
- Non-technical (e.g., the organization with security authority and responsibility)

Identifies a need to understand the dynamics between them

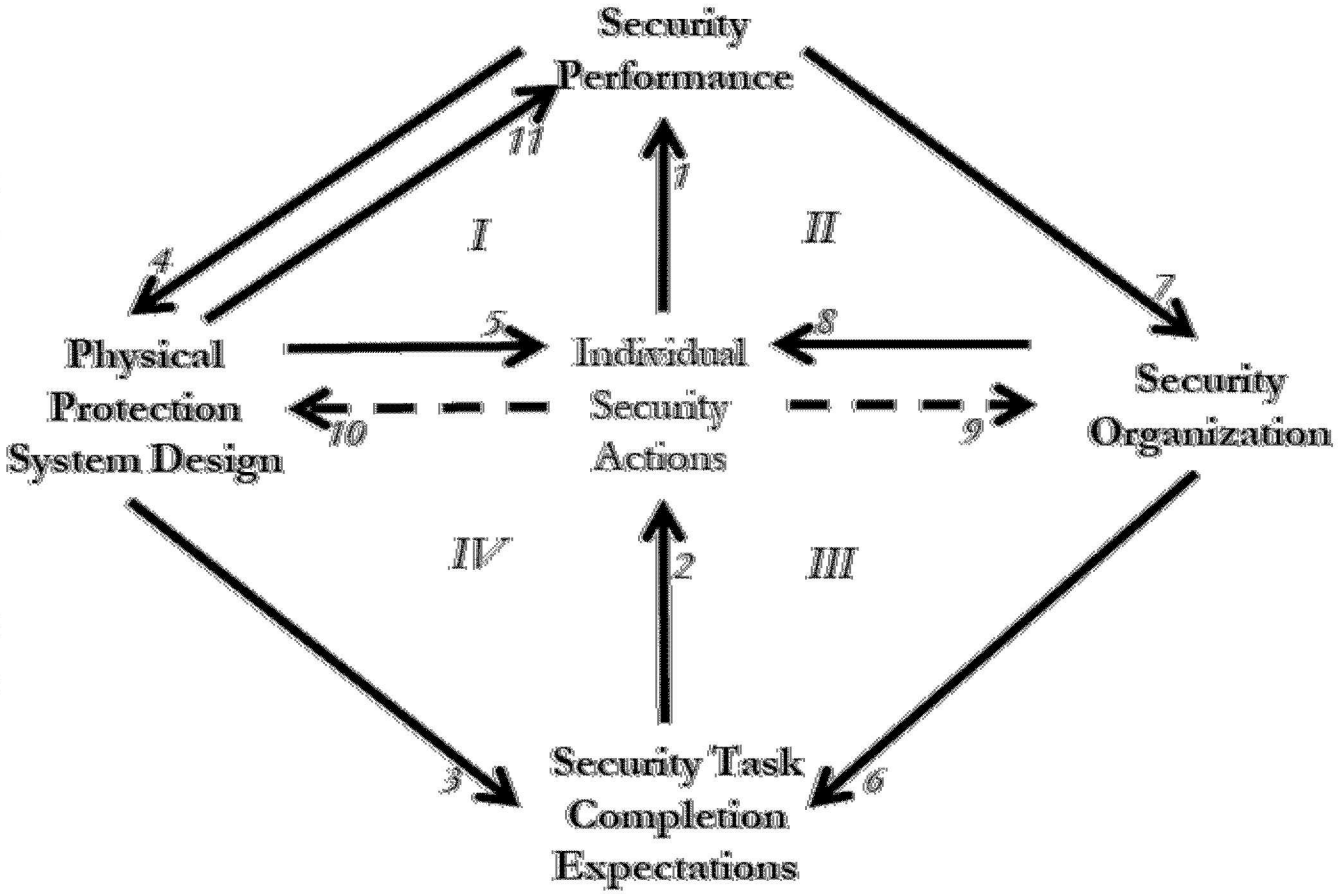
- Daily work practices affect both PPS & the security organization → ***interdependence***
- Past levels of security performance influences both PPS & the security organization (which affects current performance) → ***feedback***

Security performance can be described as "how well individual security actions achieve security functions with a given PPS design"

A New Approach: STFS (2/4)

Systems-Theoretic Framework for Security (STFS)

- Consistent with tenet ***engineering system complex systems analysis***



- Elements (text), links (Arabic #s), & feedba loops (Roman numer ***describes security performance***

- Provides a ***structured thought process on how socio-technical interactions*** affect individual/collective behaviors & security performance

A New Approach: STFS (3/4)

Logic:

- High-quality ***completion of security tasks*** envisioned by the PPS is necessary to accomplish high level security functions

Security task completion consists of 3 behavioral performance requirements:

- The required task is identified and assigned
- The standard for the task is met
- Meeting these standards of task completion is sufficient to achieve primary PPS security functions

STFS illustrates how ***dynamic, socio-technical interactions*** influence the ***validity*** of these 3 requirements

A New Approach: STFS (4/4)

STFS can help identify where organizational influences can cause security task completion to vary significantly from expectation

Example:

- Facility A → internal security assessments meet requirements + strong preventive PPS maintenance program
- Facility B → internal security assessments meet requirements + (almost daily) maintenance necessary for portions of PPS to be operational
- Facility A is expected to have better security performance than Facility B (with the same PPS)

STFS can help designers & assessors of security performance identify non-traditional areas of improvement

- Illustrating role of organizational influences on traditional PPS measures
- Emphasizing importance of the quality of security task completion
- Levers of influence over assumptions on human behavior

Contributions (1/2)

Theoretical Contributions

- Supports security as an ***emergent property of complex systems***
- Introduces **security task completion** for socio-technical interactions

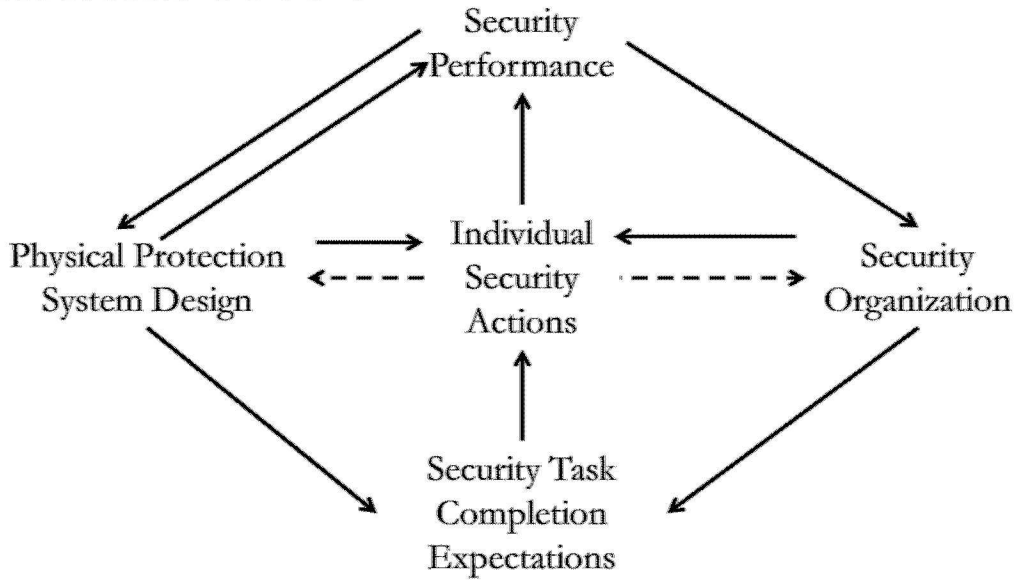
Methodological Contributions

- Shifts security focus to ***balancing*** socio-technical dynamics
- Incorporates ***patterns of practice*** in security performance

Practical Contributions

- Offers a ***graphical model for socio-technical interactions*** in security
- ***Provides one link*** between DEPO & nuclear security culture model
- Includes a ***broader set of features in security*** performance to
  - (1) enhance PPS design methods, (2) update security procedures or (3) improve security inspection checklists

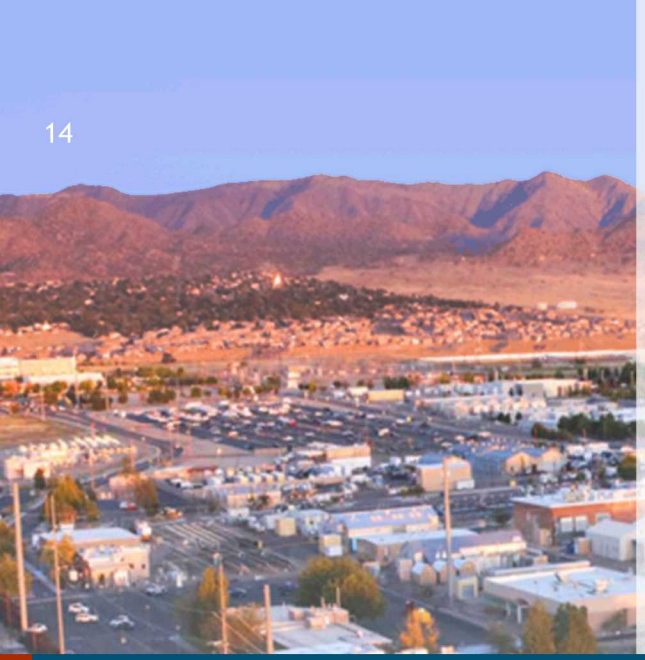
Contributions (2/2)



STFS could provide a starting point for the ***total systems approach*** called for in a 2011 National Academies study "Understanding and Managing Risk in Security Systems for the DOE Nuclear Weapons Complex "

STFS helps describe whether ***the human elements of this complex system*** can accomplish ***security tasks with the level of quality*** envisioned by PPS designers

STFS offers a ***structured thought process for how socio-technical interactions*** affect security performance at nuclear facilities



QUESTIONS?