SAND2019-7983C

# Socio-Technical Interactions: A New Paradigm for Nuclear Security

*PRESENTED BY*

Adam D. Williams

60th Annual Meeting of the Institute for Nuclear Materials Management

14-18 July 2019

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.

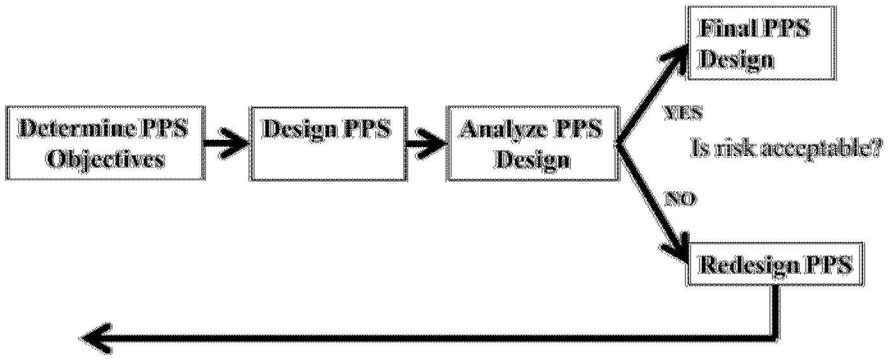
# Outline

- Introduction
- Insights from a Multidisciplinary Literature Review
- The Need for a New Approach to Nuclear Security
- Conclusions

# Introduction

## Technology-Based Approaches

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




Tend to generate ***same*** PPS design before/after significant shift in

- Corporate culture
- Organizational structure
- Personnel turnover

## Human-Based Approaches

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


Describes variance in nuclear security as resulting from social—rather than technical—changes:

- Management systems
- Leadership behaviors
- Personnel Behaviors

# Introduction

<u>According to a former NNSA Chief of Defense Nuclear Security</u>:
1983 transition in ownership of security at Savannah River Site

- Noted distinct difference in security performance between oversight entities
  - DuPont = overly cautious/occupational safety conscious culture → limited the security success
  - Wackenhut = the action and accountability-oriented philosophy → strong performance

- ***Dupont example***, during a security force training course on hostage rescue (recapturing a reactor control room from adversaries)
  - "when it was time to dispatch the special response team, the security managers would not do so, on the argument that it was too dangerous"

- ***Wackenhut example***, shortly after this change, there was a night time perimeter fence alarm near one of the reactors
  - "the security personnel scrammed the reactor, removed the operators, called the SRT and local law enforcement and then conducted an 'inch-by-inch search' of the facility
  - 'Though we never found anything…the serious response was a great experience.'

Suggests a need to reconcile how the ***same nuclear facility*** with ***two different operators*** can have ***different security performance***

# Multidisciplinary Literature Review

Traditional focus on ***technological solutions*** (like in DEPO) based on the assumption that ***any task*** necessary for successful PPS will be completed:

- Adequately
- With high quality

This is a simplifying and untenable assumption that ***negates the impacts of non-technical influences*** on security performance

Extensions to DEPO demonstrate that non-technical influences can be modeled as:

- Influences on control over PPS components [Nunes-Vaz & Lord,, 2014]
- Organizational influences on accomplishing PPS functions [Argenti, et al., 2017]

Yet, do not full reconcile common refrain from former Department of Energy security czar Gen. Eugene Habiger:

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

# A New Approach

| | ***Actual security operations = Expected security operations*** | ***Actual security operations ≠ Expected security operations*** |
|---|---|---|
| ***Adequate PPS Design (~$P_E$)*** | Adequate security procedures<br>Strict adherence to related procedures<br>**STRONG Performance** **(A)** | Adequate security procedures<br>Deficient adherence to related procedures<br>**WEAK Performance** **(B)** |
| ***Inadequate PPS Design (~$P_E$)*** | Inadequate security procedures<br>Strict adherence to related procedures<br>**WEAK Performance** **(C)** | Inadequate security procedures<br>*"Going beyond" adherence to related procedures*<br>**STRONG Performance**<br>Inadequate security procedures<br>*Deficient adherence to related procedures*<br>**WEAKEST Performance**<br>**(D)** |

# A New Approach

| | ***Actual security operations = Expected security operations*** | ***Actual security operations ≠ Expected security operations*** |
|---|---|---|
| ***Adequate PPS Design (~$P_E$)*** | Adequate security procedures<br>Strict adherence to related procedures<br>**STRONG Performance** **(A)** | Adequate security procedures<br>Deficient adherence to related procedures<br>**WEAK Performance** **(B)** |

Top row = DEPO-based approaches focus on technical PPS performance

- Tend to assume strict adherence to adequate security procedures

Quadrant A = ***strong performance*** = adequate PPS + strict adherence

Quadrant B = ***weak performance =*** adequate PPS + insufficient adherence

Quadrants A and B ***commonly accepted***

# A New Approach

| | ***Actual security operations = Expected security operations*** |
|---|---|
| ***Adequate PPS Design (~$P_E$)*** | Adequate security procedures<br>Strict adherence to related procedures<br>**STRONG Performance** **(A)** |
| ***Inadequate PPS Design (~$P_E$)*** | Inadequate security procedures<br>Strict adherence to related procedures<br>**WEAK Performance** **(C)** |

Left-hand column = IAEA nuclear security culture model-based encouragement of adherence

- Tend to assume the existence of an adequate PPS

Quadrant A = ***strong performance*** = adequate PPS + strict adherence

Quadrant C = ***weak performance = in***adequate PPS + sufficient adherence

# A New Approach

New, non-traditional possible outcomes:

- Quadrant C = ***weak performance*** = Inadequate PPS + strict adherence
- Quadrant D* = ***strong performance*** = Inadequate PPS + deficient adherence (compensate)
- Quadrant D* = ***weak performance*** = Inadequate PPS + insufficient adherence (deficient)

| | | |
|---|---|---|
| ***Inadequate PPS Design (~$P_E$)*** | Inadequate security procedures<br>Strict adherence to related procedures<br>**WEAK Performance** **(C)** | Inadequate security procedures<br>*"Going beyond" adherence to related procedures*<br>**STRONG Performance**<br>Inadequate security procedures<br>*Deficient adherence to related procedures*<br>**WEAKEST Performance** **(D)** |

# A New Approach

2x2 matrix shifts between ***static image*** of & ***dynamic changes*** in the drivers of security performance

- Behaviors ***in the moment*** that result in strong security performance may have ***time-delayed, deleterious*** side effects on future security performance

- For example, from PPS design/installation manager:
  - *"on three different occasions during a walk-down inspection…told , "Halt, on the ground"… The security personnel were taught that, "Anything other than nothing going on is off-normal" and requires an immediate response—including up to a complete facility lockdown.*

- Security personnel showed strict adherence to adequate protocols (quadrant A) that resulted in strong security performance ***at the time***—

- Over time repetitively forcing inspectors to the ground wastes resources & undermines cooperation ***potentially leading*** to quadrant B

# A New Approach

This matrix provides a way to organize the relationships between

- PPS adequacy
- Security operations
- Adherence to procedures
- Security performance

***If*** adherence to security protocols drives strong security performance, ***then***:

- Need to identify ***designable*** & ***controllable influences*** on adherence
- Build on core attributes of engineering systems [de Weck, et al., 2011] to better explain manage these socio-technical interactions

# A New Approach

Helps frame further exploration of dynamics that describe the movement within the 2x2 matrix of security performance outcomes, consistent with:

- "migration toward the boundaries of acceptable behavior" [Rasumussen, 1997]
- "normalization of deviance" [Vaugn, 1996]
- "drift into failure" [Dekker, 2011]
- "system migration toward states of higher risk" [Leveson, 2012]
- mapping continuous improvement [IAEA, 2014] as movement between Quadrant A to the strong interpretation of Quadrant D (and back)
- identifying milestones (positive) or benchmarks (negative) to changes in nuclear security performance

# Conclusions

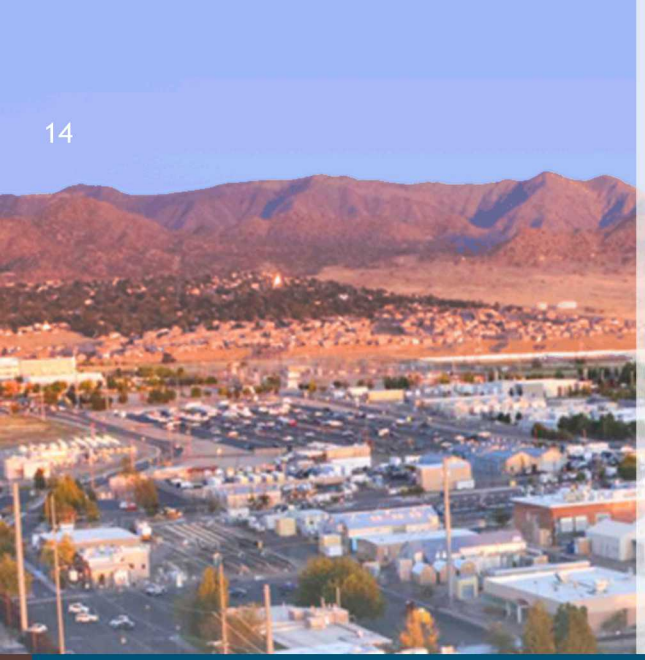
Socio-technical systems approach offers new insights for nuclear security

- Security performance is a ***system-level property*** that requires both
  - Technical reliability of the PPS (rows of the matrix)
  - Behavioral quality of security personnel (columns of the matrix)
- Technical reliability & behavioral quality ***interactions*** → different outcomes

The matrix implies

- Security performance is ***not a static attribute*** of nuclear facilities
- A shift from optimizing PPS toward ***equilibrating socio-technical*** interactions
- Security performance = individuals/organizations ***adjusting to realities*** of PPS

Matrix establishes a new foundation incorporating ***both*** technical and non-technical elements to better combat 21st century threats



# QUESTIONS?