SAND2021-10203C

Early Results from Applying a Multilayered Network Framework to Engineering Nuclear Security Systems

Adam D. Williams, Gabriel C. Birch, Sue Caskey, Elizabeth S. Fleming, Thushara Gunda, Thomas Adams, Jamie Wingo, Jami Stverak (Sandia National Laboratories)

INMM & ESARDA Joint Virtual Annual Meeting

August 23-26 & August 30-September 1, 2021

This work was supported by the Laboratory Directed Research and Development program at Sandia National Laboratories, 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-NA0003525.

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.

SAND2021-TBD C

Roadmap

Introduction

Key Themes from Empirical Data

From Empirics to Multilayered Networks

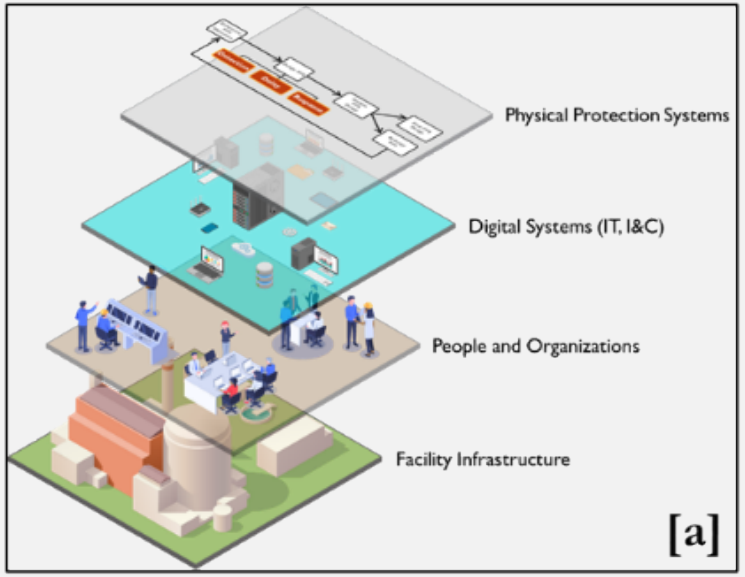
Multilayered Network Model Results

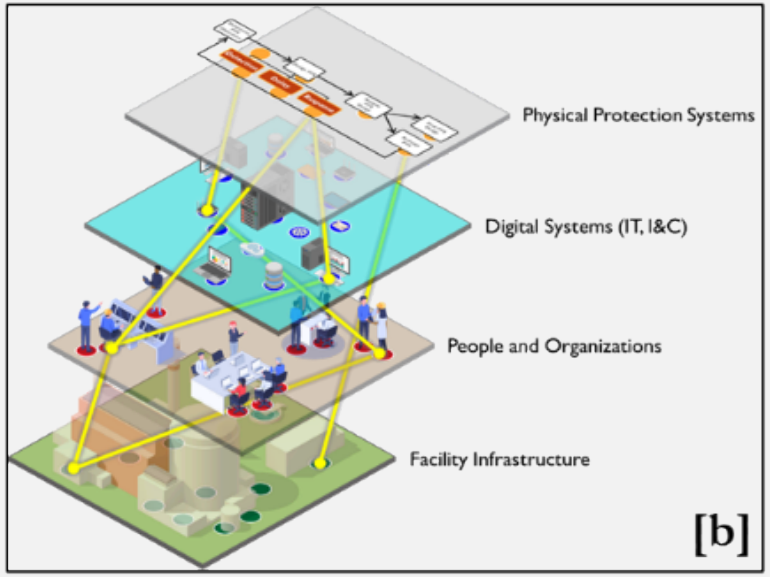
Insights, Implications & Future Work

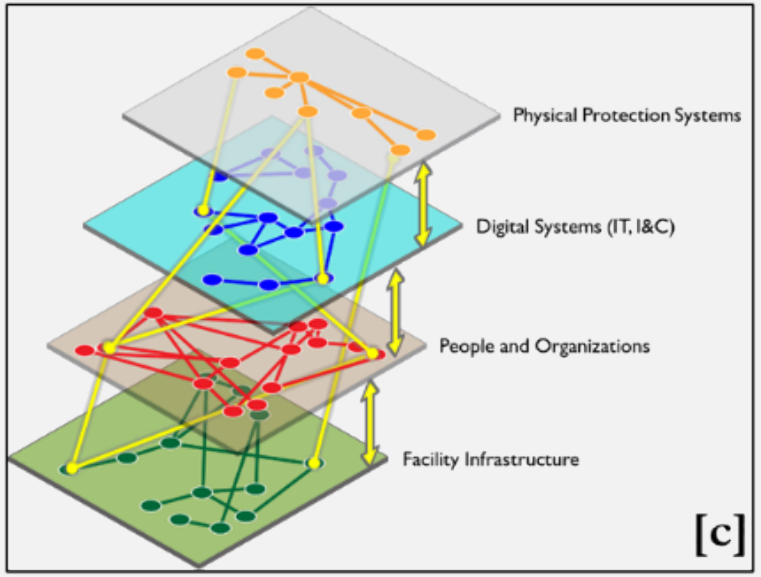
Introduction

- Dynamic trends increase *complexity* for nuclear security

- Response → Reframes security engineering multidomain interactions



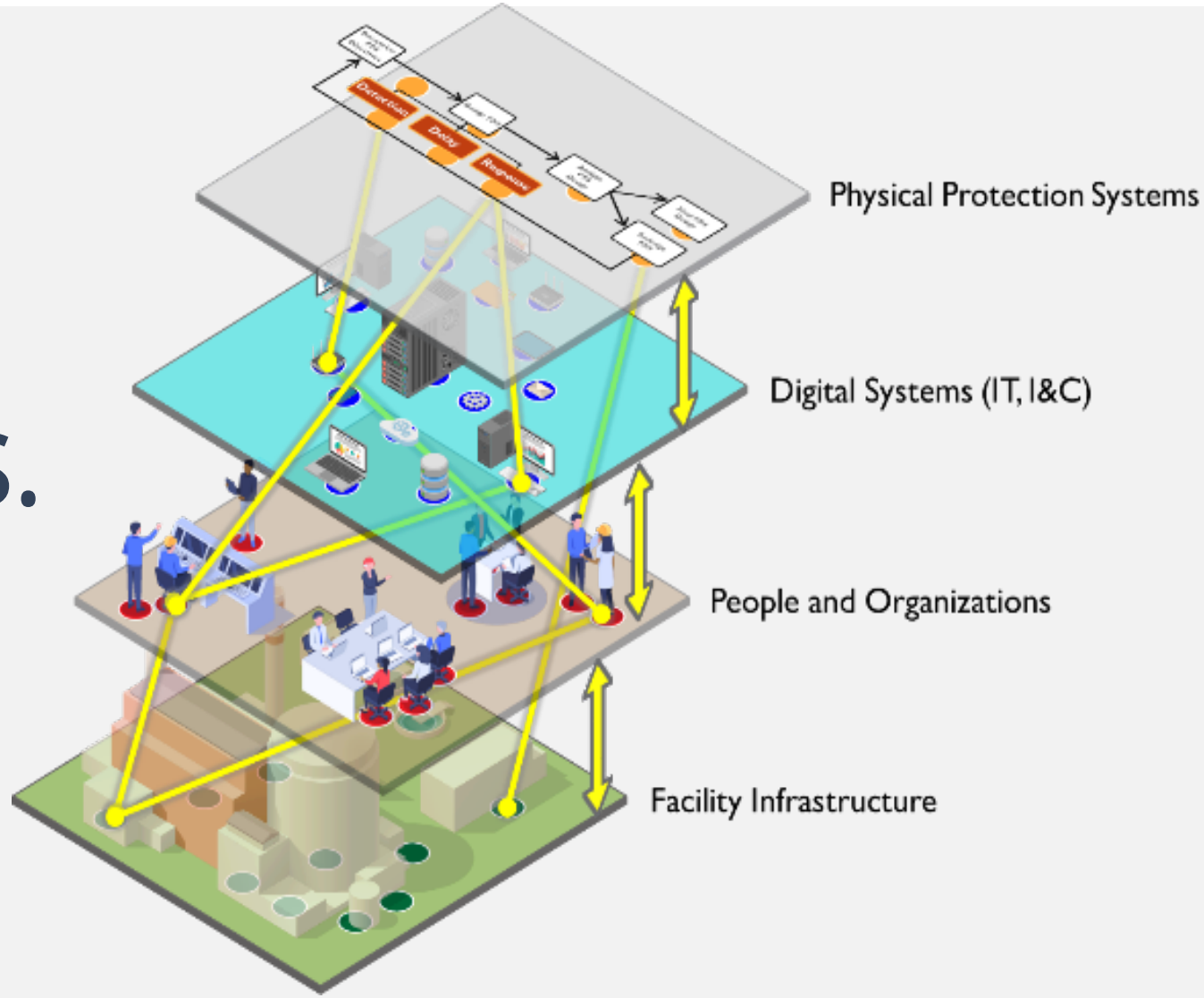




Introduction

- Disparate, ‘individual’ security mitigations
  - Cyber security via common vulnerability scoring system
  - Physical security via “gates, guards, guns”
  - Personnel security via human reliability programs
- These are often assumed independent!

VS.

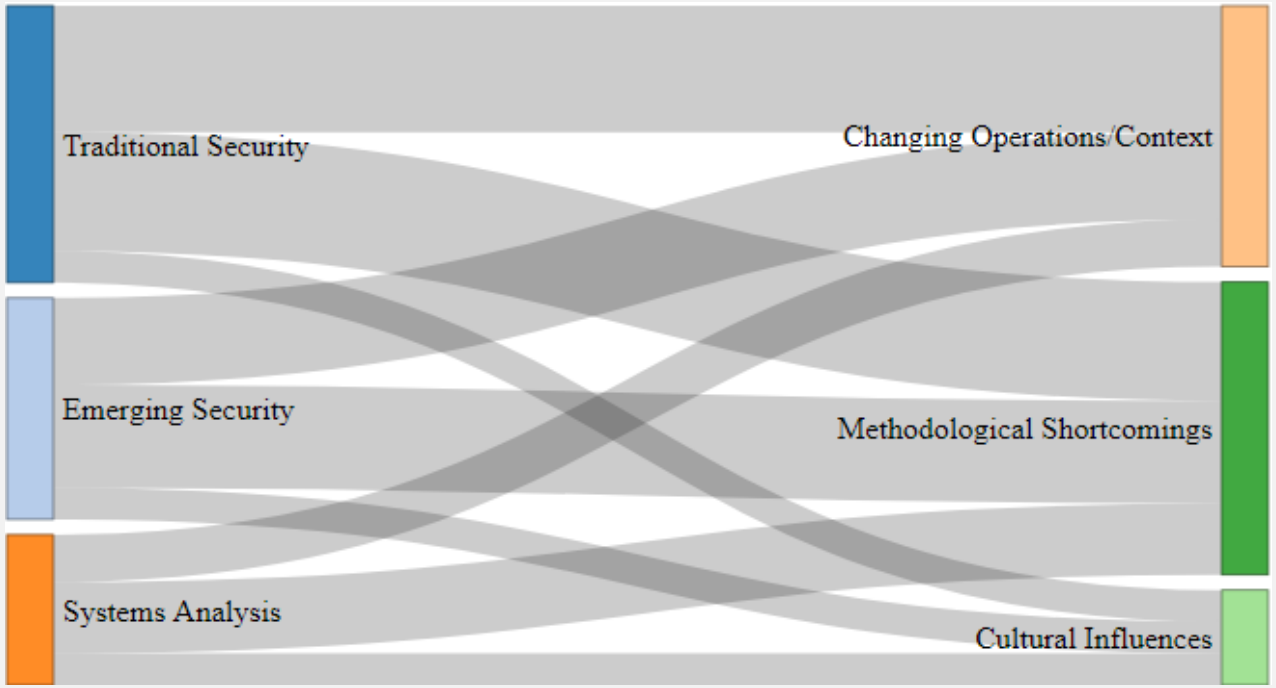


•Key Themes from Empirical Data

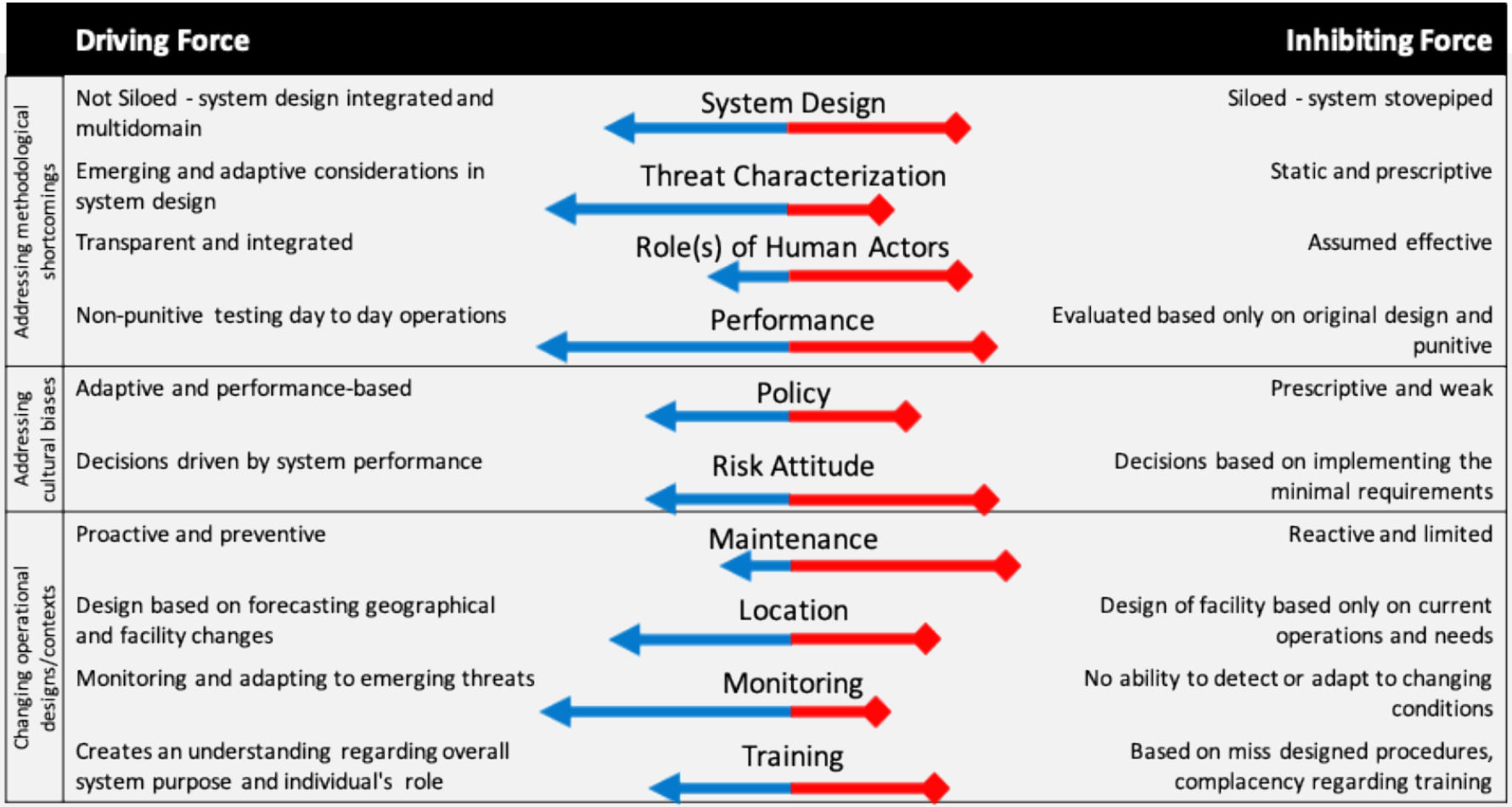
Nuclear Security World View	Description
Traditional Security	Experts involved in execution of traditional security analysis or designs domestically or internationally, ranging from analysis to management activities.
Emerging Security	Experts involved in developing new tools, technologies, or paradigms within nuclear security (including cybersecurity), noting that most of these experts have experience implementing current HCF approaches.
Systems Analysis	Experts who shared a common perspective of systems-based approaches and formal analytical backgrounds despite working in such diverse applications as resilience, human cognition, and security analysis.

- Data Collection (29 subject matter experts, interviews & focus groups)
- Worldviews → common models of system philosophy & practice (from INCOSE)
  - Leverage key insights across different areas
  - Defined on overall perspective

- Data Analysis = Key insights + major themes
- Sankey Diagram → map of relationships between key concepts
  - Data across worldviews → themes more likely to be reliable, valid, and generalizable



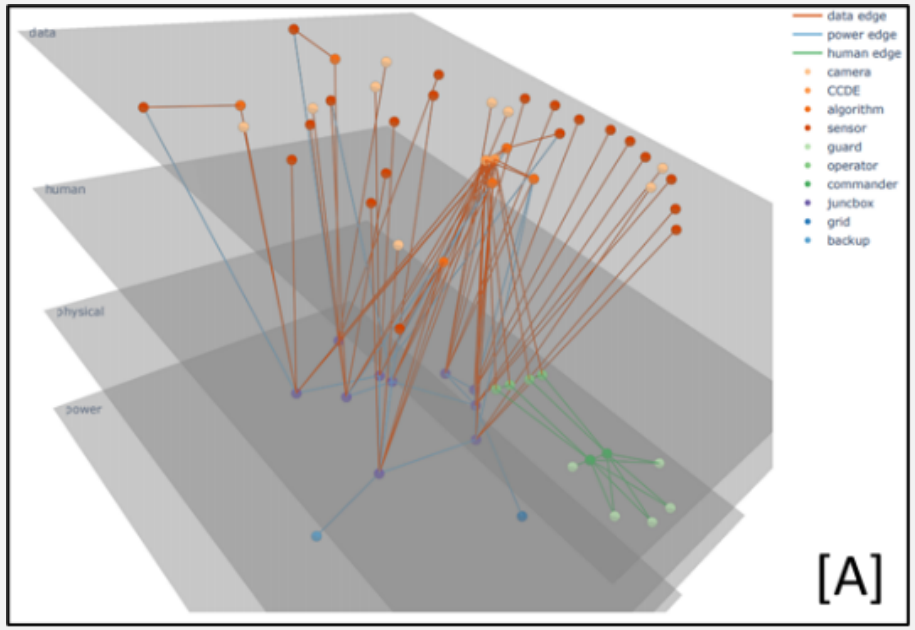
•Key Themes from Empirical Data

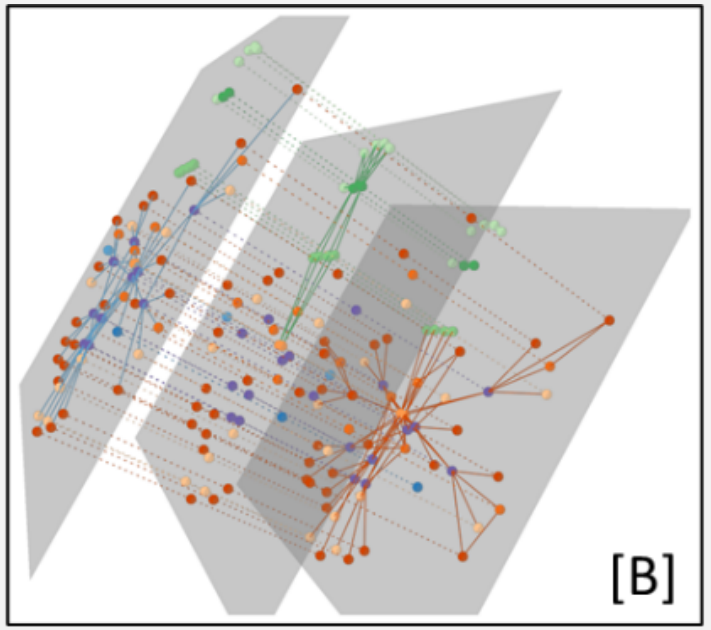


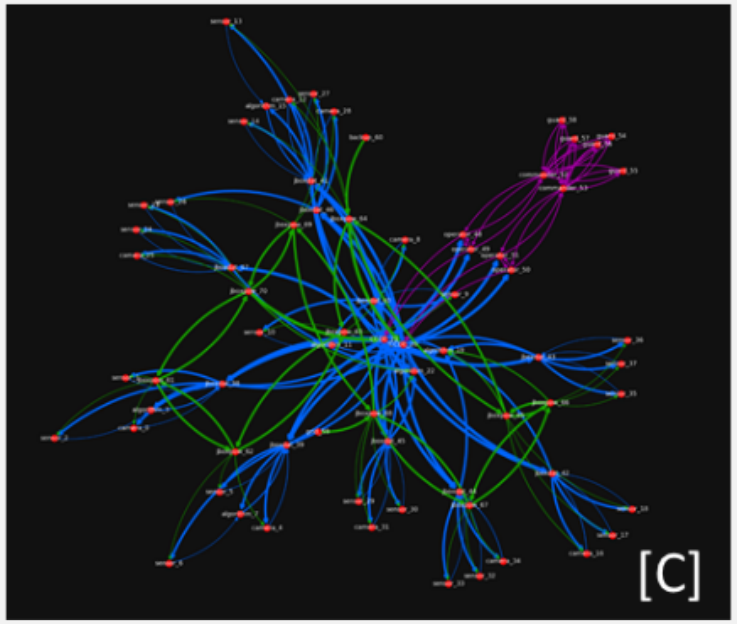
	Driving Force		Inhibiting Force
Addressing methodological shortcomings	Not Siloed - system design integrated and multidomain	System Design	Siloed - system stovepiped
	Emerging and adaptive considerations in system design	Threat Characterization	Static and prescriptive
	Transparent and integrated	Role(s) of Human Actors	Assumed effective
	Non-punitive testing day to day operations	Performance	Evaluated based only on original design and punitive
Addressing cultural biases	Adaptive and performance-based	Policy	Prescriptive and weak
	Decisions driven by system performance	Risk Attitude	Decisions based on implementing the minimal requirements
Changing operational designs/contexts	Proactive and preventive	Maintenance	Reactive and limited
	Design based on forecasting geographical and facility changes	Location	Design of facility based only on current operations and needs
	Monitoring and adapting to emerging threats	Monitoring	No ability to detect or adapt to changing conditions
	Creates an understanding regarding overall system purpose and individual's role	Training	Based on miss designed procedures, complacency regarding training

- Force field diagram (FFD) → balancing positive & negative forces
- Forces *either* drove behavior *toward* the ideal state or *inhibited* change

FROM EMPIRICS TO MULTILAYERED NETWORKS







- Node Layer [A] → simplified visuals as smaller connected networks by node type
- Replica Node [B] → visualizes all nodes on each layer, distinguishes each layer by node category
- Aggregate Network [C] → flattens multiple layers into a single 2-D representation

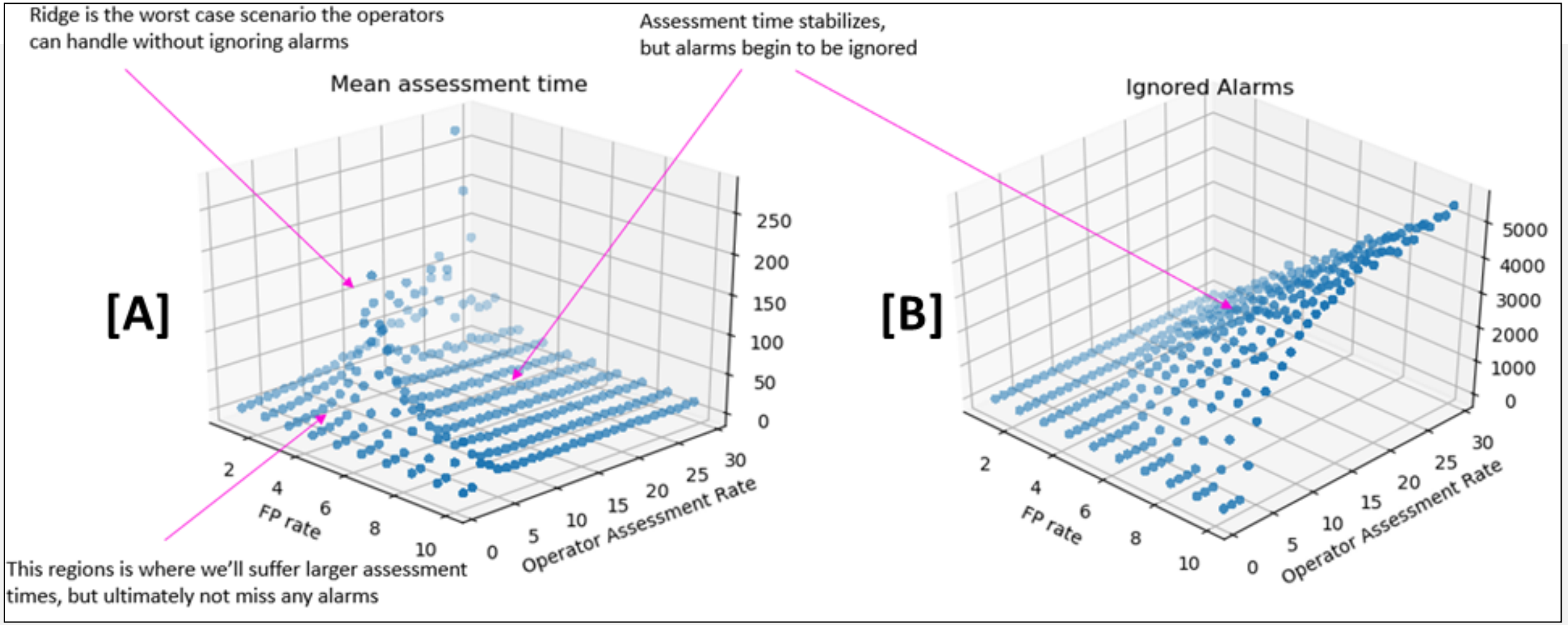
•Multilayered Network Model Results

- Experiment 1: MLN model of simplified 10-sector hypothetical security system
  - 60 nodes and 216 edges between nodes and *across* security functional layers

- Other notable experimental characteristics:
  - "first in, first assessed" alarm queue strategy
  - Varied the false positive rate (1%-10%)
  - Varied operator assessment rate (1-30 time units)

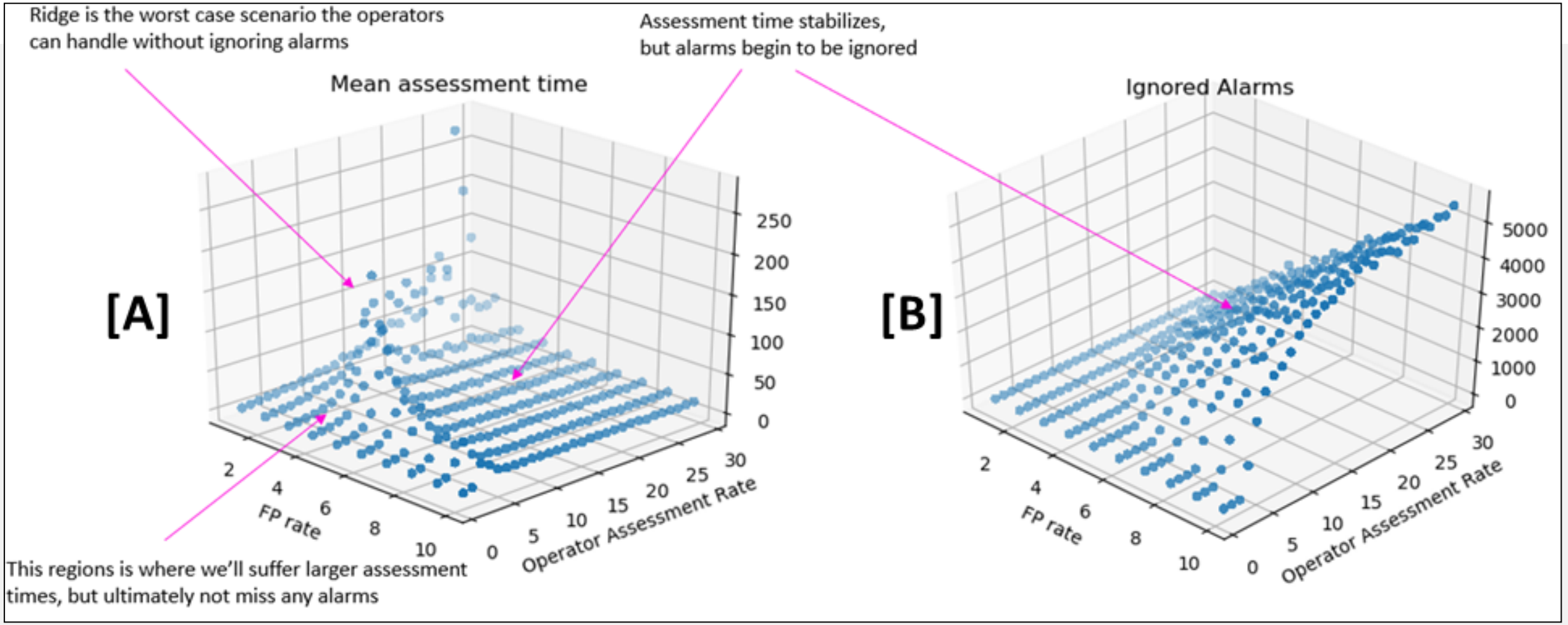
- Goal: Evaluate time between alarm & assessment, as well as # alarms lingering in queue
  - [A] Surface describing impact of varying FP & operator assessment rates on ***mean assessment time*** (Note: "worst-case" ridge)
  - [B] Surface describing impact of varying FP & operator assessment rates on ***# of ignored alarms*** (Note: low assessment times + high ignored alarms)

•Multilayered Network Model Results



- [A] Surface describing impact of varying FP & operator assessment rates on *mean assessment time* (Note: "worst-case" ridge)
- [B] Surface describing impact of varying FP & operator assessment rates on *# of ignored alarms* (Note: low assessment times + high ignored alarms)

•Multilayered Network Model Results



- If either operator assessment speed is slowed or sensor false positive rate is increased, alarms will begin to be ignored (intuitive)
- Non-linear relationship between false positive rate, operator assessment time, & number of ignored alarms (non-intuitive)
- MLN produces a mathematical description that matches intuition/observation & is beyond current security system approaches

Insights, Implications & Future Work

Insights

- Including cross-domain interactions → comprehensive model of security
- MLNs models → transition from “reactive” to “proactive” security paradigm

Implications

- “Worldview” agreement on need for more systemic processes & models
- MLN models combine complex systems principles with network math

Future Work

- Incorporating high(er) fidelity models for the role(s) of human actors
- Advanced MOD/SIM, validation & benchmarking


QUESTIONS???