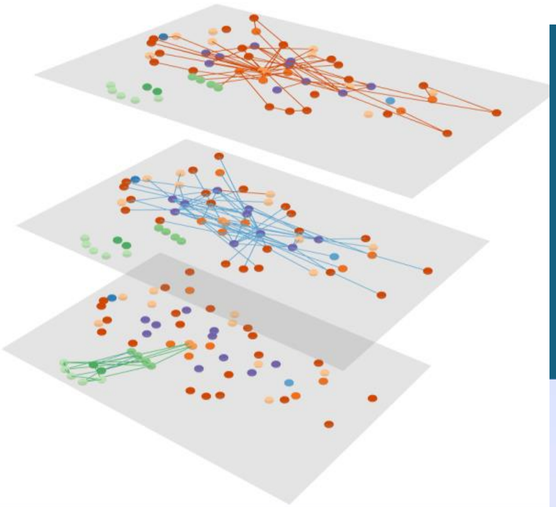
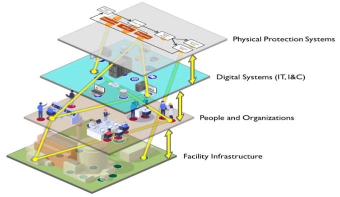
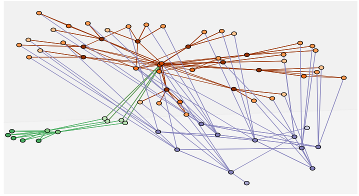
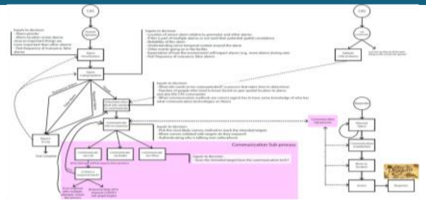
Insights for Systems Security Engineering from Multilayer Network Models









PRESENTED BY

Adam D. Williams, Gabriel C. Birch, Susan A. Caskey, Elizabeth S. Fleming, Thushara Gunda, Jamie Wingo, & Thomas Adams

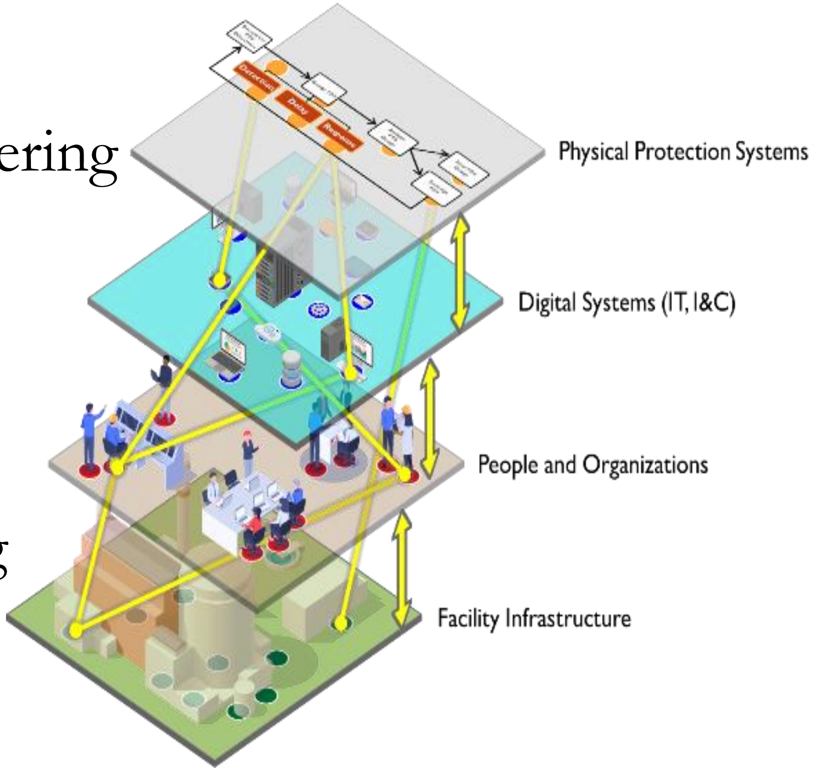
INCOSE International Symposium

July 2021

SAND2021-4018 C 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
- A Multilayer Network Approach for Systems Security Engineering
- Multilayer Network Results for Systems Security Engineering
- Multilayer Network Insights for Systems Security Engineering



Introduction

Dynamic trends increase ***complexity*** for high consequence facility (HCF) security

- Complex risk environment-based challenges
- Adversary innovation-based challenges
- Disruptive technologies-based challenges

2018: Increased digitization of control elements in HCF	**2020: Nuclear facilities deployed to increasingly remote locations**
2019: Cyber attack on Indian Kudamkulam Nuclear Power Plant	**2011: DHS memo "violent extremists… insider positions"**
2019: Yemeni rebels use UAS to attack Saudi Oil facilities	**2020: Expected threat from deep-fakes & malicious AI**

Result → challenge to efficacy of current HCF security paradigms

Response → Sandia LDRD research reframes systems security engineering

- Interactions matter!
- Multidomain interactions of HCF security modeled as connections between network layers
- High consequence facility (HCF) security → complex system behavior

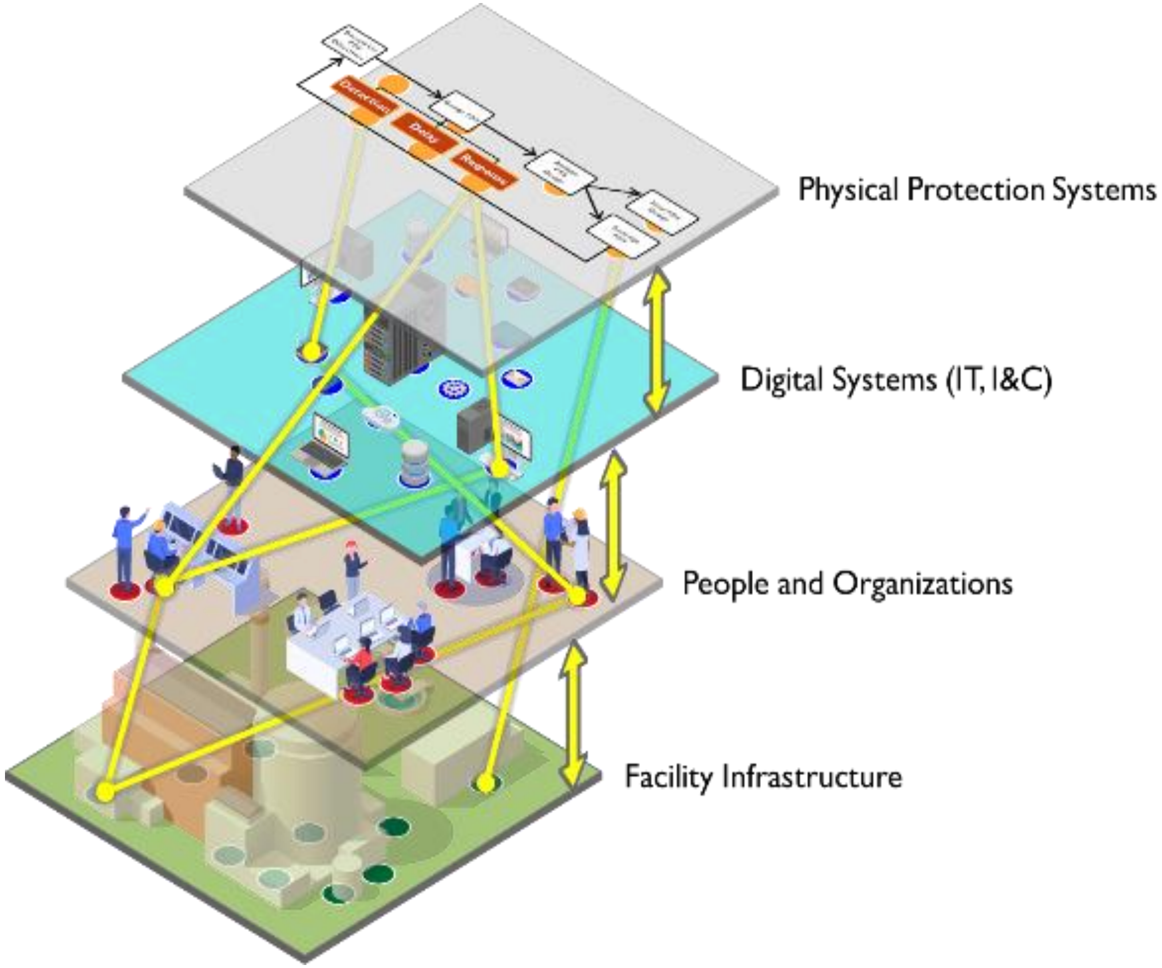
Multilayer Network Approach

Disparate, 'individual' security mitigations

- Cyber security via common vulnerability scoring system
- Physical security via "gates, guards, guns"
- Personnel security via human reliability programs

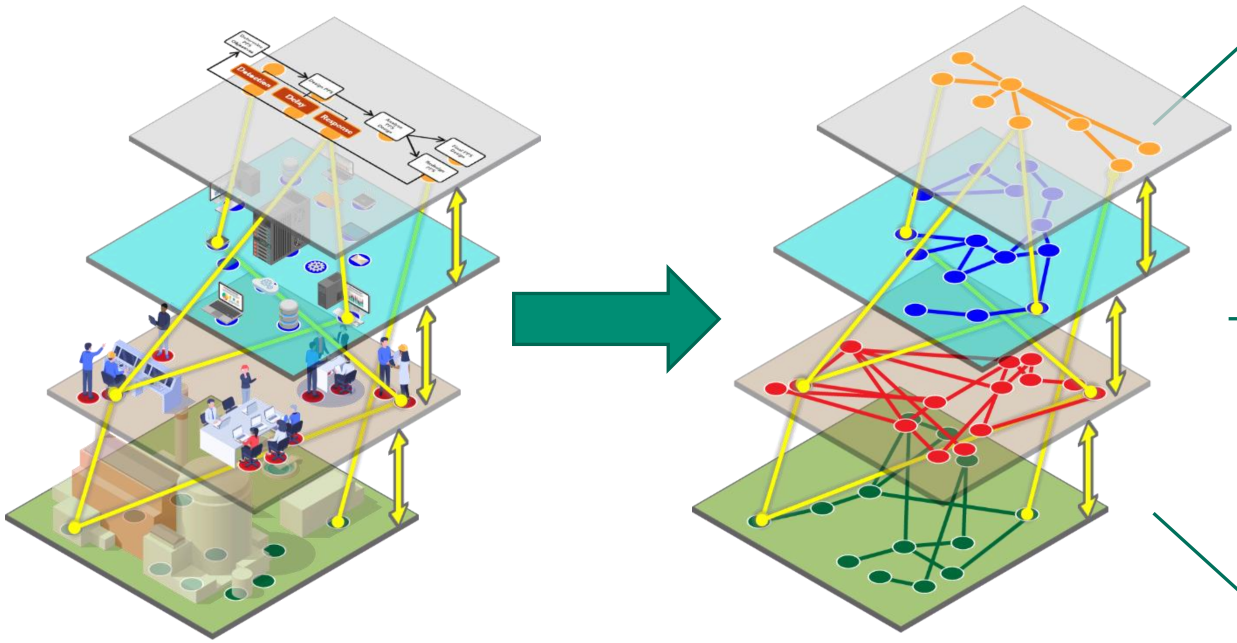
These are often assumed independent!

VS.



Multilayer Network Approach: Multidisciplinary Foundations

Multidisciplinary Foundations



Complexity Theory

- Attempt to reconcile unpredictability of dynamic systems with a sense of order & structure
- Non-linear cause/effect as parallel processes because “meaning is achieved through connections”
- Many, simple interacting components → complex, unexpected performance

Systems Theory

- Non-statistical, non-random logic to describe the behaviors of “many, but not infinitely many”
- Behaviors → equilibrium of initial conditions, boundary constraints & external disturbances
- Systems naturally migrate toward states of greater disorder without counteracting forces

Network Theory

- Identify/analyze interactions between components that produce non-linear behaviors
- Describes how relationships between nodes result in observed, higher-level behaviors
- Components *within* and *across* layers can interact and result in unexpected—yet, potentially designable—behaviors

Multilayer Network Approach: Empirical Support

HCF Security Worldview [Representative expertise]	Subject Matter Experts [Total #]	Training [# per type]	Years [Range]
Traditional Security [Vulnerability analyses & HCF physical implementation]	7	Formal [3] Informal [4]	>5 to >30 (FG1 2 to 7 years)
Emerging Security [Security mod/sim; Physical security requirements at HCF]	6	Formal [3] Informal [3]	>2 to >20
Systems Analysis [Resilience & analysis; Threat & consequence analysis]	7	Formal [2] Informal [5]	>2 to >15 (FG2 2 to 30 years)

Data Collection

- 29 SMEs across HCF security-related disciplines
- Qualitative, open-ended interviews & focus groups

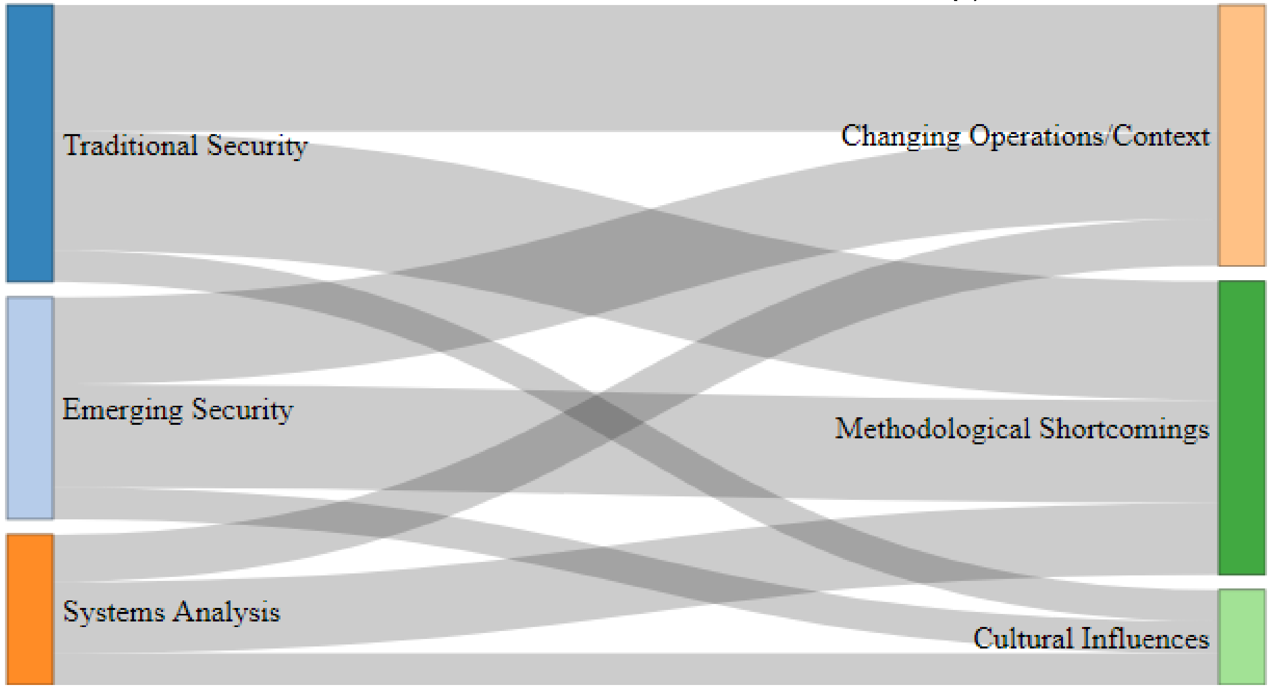
Worldviews → common models of system philosophy & practice (from INCOSE)

- Used to leverage key insights from SMEs across different areas of expertise
- Defined based on the SME's overall per-spective (rather than only their current HCF security role or set of responsibilities)

Multilayer Network Approach: Empirical Support

Data Analysis = Key insights + major themes

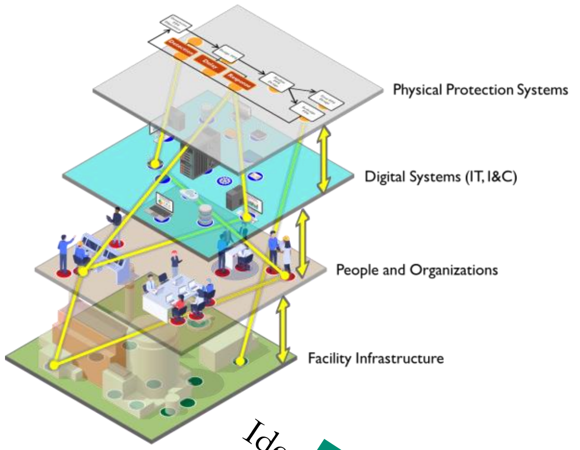
- Themes → patterns of similarities in data related to current challenges & future needs of HCF security



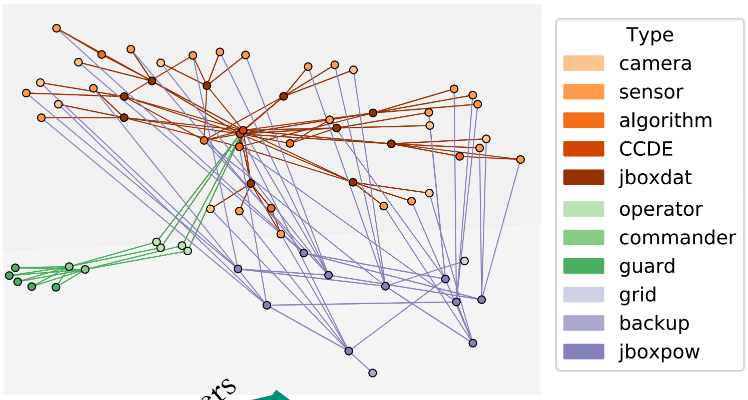
Sankey Diagram → robust and easy-to-understand map of relationships between key concepts

- Spread of the data across worldviews → themes more likely to be reliable, valid, and generalizable

Multilayer Network Approach: Model Development

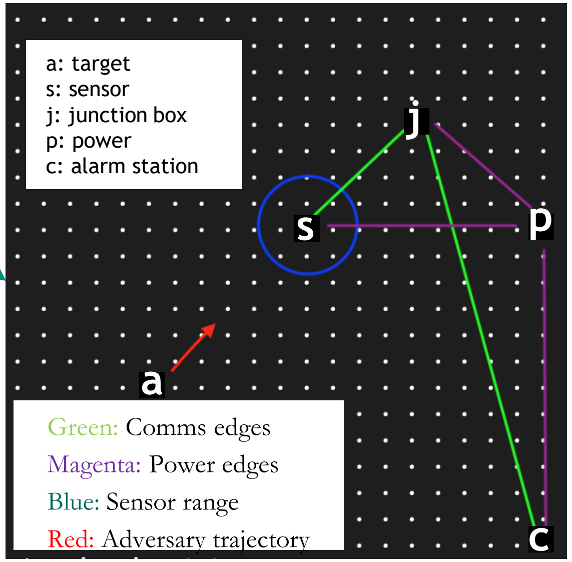


Identify/arrange components per layer



Connect components between layers

Into Continuous Time Markov Chain Sim



Layer Name	Conceptual Function (HCF security measure)	Network Representation (example HCF security component)
Data & Communications	Capture data flows/Detection	• Data generators (microwave sensors) • Data receivers (operators or control systems)
Supporting Infrastructure	Provide power, temperature control, structure/Detection, Response	• Power provider (junction boxes)
Human actors	Various roles of human actors/Detection, delay, response	• Humans (command system operator, security manager)

LDRD

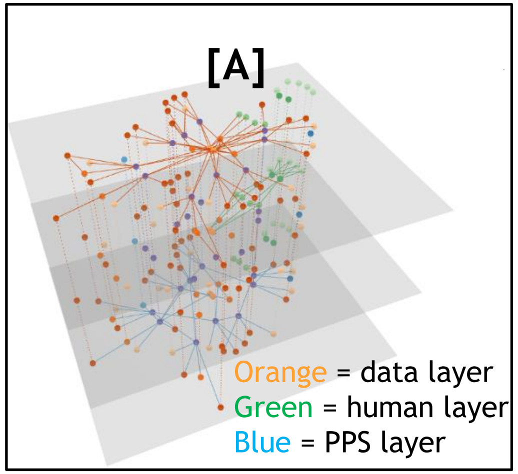
Multilayer Network Results

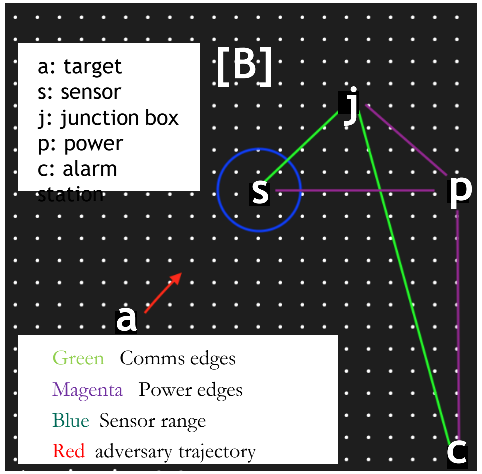
[A] MLN-based model consisting of user defined number of:
- Technical elements: sectors, sensors, junction boxes
- Non-technical elements: human operators, policies

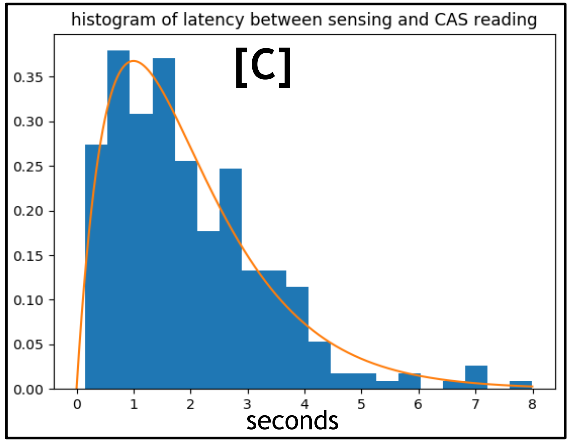
[B] MLN-based simulation in which:
- An adversary (denoted as "a") moves towards a sensor (denoted as "s")
- "s" has detection range as the blue circle & is connected via communication edges (green lines)
- "s" signals move through a junction box (denoted as "j") to security central alarm station (denoted as "c")
- A power node (denoted as "p") provides electricity (purple lines) to all technical elements

[C] MLN-based simulation able to
- Correctly identify & communicate the presence of an adversary
- Capture scenarios where sensors failed to report adversary target presence because of
  - the probabilistic description of sensor detection reliability
  - inadequate power was provided
- Define the latency (measured in seconds) between detection & messages arriving at the central alarm station

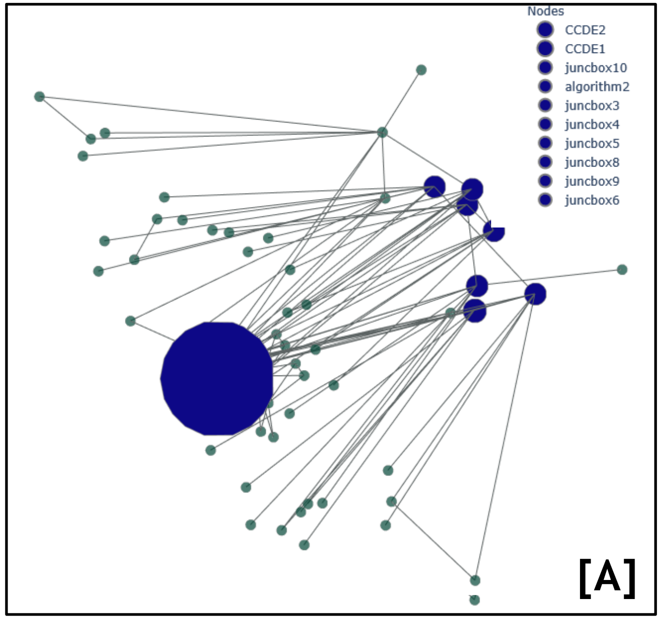
[C] Demonstrates **two useful capabilities** for systems security engineering:
- Ability to capture impacts of underlying system infrastructure
- Timing dynamics between sensors & humans

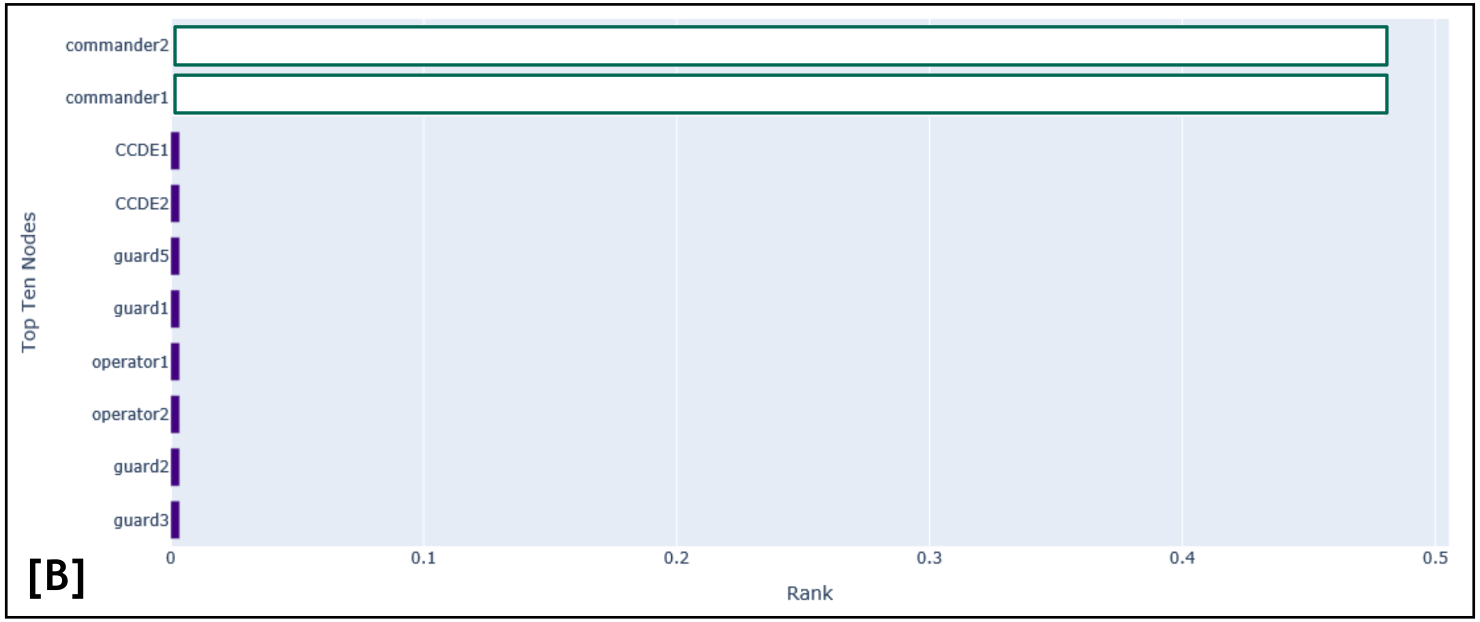






Multilayer Network Results





Applying MLN mod/sim to a (still relatively simplified) 10-sector hypothetical HCF security system → 60 nodes and 216 edges between nodes and *across* security functional layers

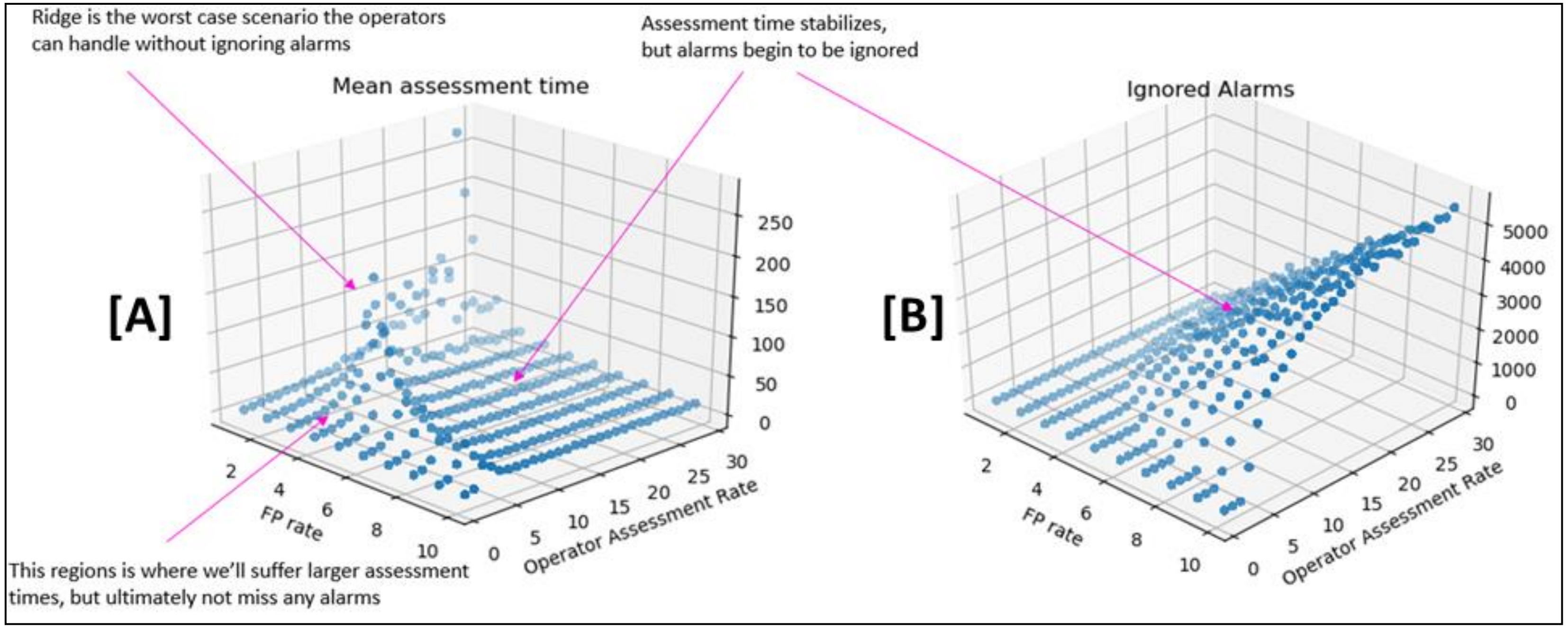
- [A] Network-graphical representation of additive page rank analysis
  - Node size is proportional to the relative importance of a node in its own layer ***as enhanced by its centrality in another layer***

- [B] Bar chart of most important MLN nodes, based on additive page rank analysis

Result:

- Communication & control display equipment (CCDE) systems are ***most important*** technical elements (intuitive)
- Junction boxes were ***second most important*** technical elements (non-intuitive)

Multilayer Network Results



Experiment 1: based on "first in, first assessed" alarm queue strategy, vary the false positive rate (1%-10%) & operator assessment rate (1-30 time units) → 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)

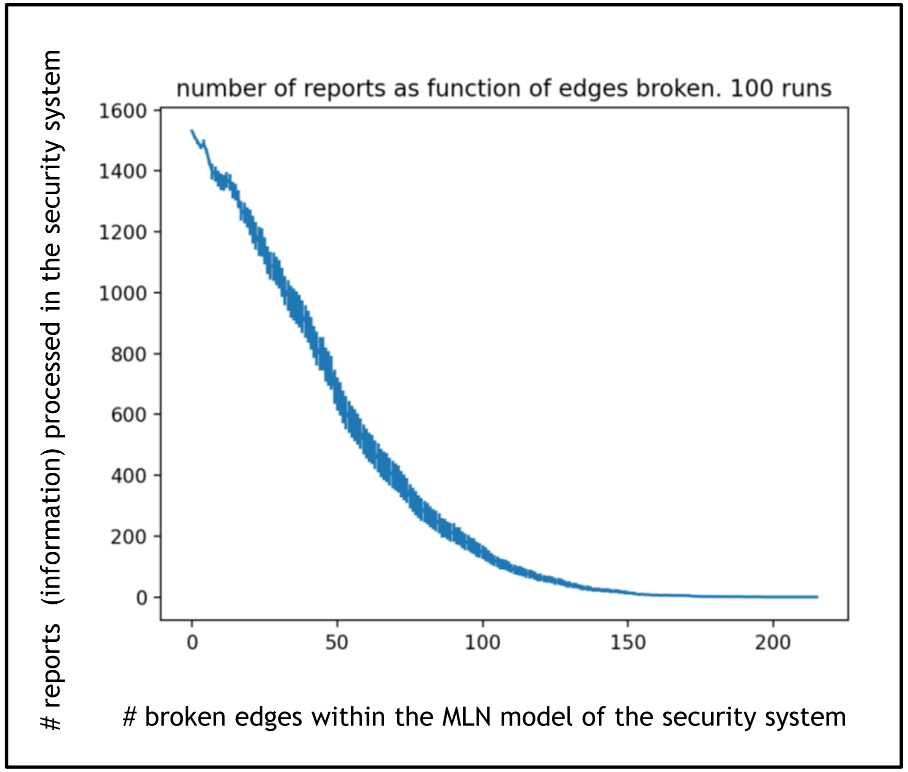
Result:

- 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
- MLN produces a mathematical description that matches intuition/observation & is beyond current security system approaches

Multilayer Network Results

Experiment 2: determine the percentage of removed edges that result in a MLN model security system failing to report any sensor alarms

- Randomly removed a MLN edge—whether *inter* or *intra-layer*—every 500 time steps
- Simulation allowed to stabilize during the ensuing 500 time steps (until a new random edge was removed)
- NOTE: "random" removal of edges could result from:
  - Accidental component failures (or misbehavior)
  - Intentional malfunctions
  - A combination of the two



Result:

- Non-linear relationship between # of randomly removed MLN model edges & total alarms received (lose 50% edges = 10% system functionality)
- MLN topology drives the location of the "tipping point" where one additional removed edge causes catastrophic system performance degradation
- Matches intuition & introduces new metric for resiliency of proposed systems security designs

Multilayer Network Insights

Key Systems Security Engineering Takeaways (Dove and Willet, 2020)	Metrics Defined by SMEs [Total number of SMEs]	Relationship(s) to Multilayer Network Metrics
Agile Security is necessary to contend with agile attack	Level of delay (time) based on defined threat (e.g. DBT) [4]	Interlayer edge with detection, intralayer edge with human layer
	Change in delay (time) versus an emerging threat [3, FG1]	Sensitivity analysis of interlayer and nonlinear intralayer edges
	Security as system failures, current/new threats [4, FG1]	***Related to multilayer network centrality, cascading metrics***
Social interactions among human and non-human system and process resources needs strategy attention	Speed/Reliability/Redundancy in interpretation of provided security information [9]	Behaviors from interlayer (e.g., decision-making) and intralayer edges (e.g., data transmission)
	Interactions between security components (e.g., detection to transmission to interpretation to human response [8])	***Intralayer edges between data and network layers (e.g., signal reliability) and data and human layers (e.g., interpretation)***
	Time from initial detection to interdiction vs. time for threat to achieve goal [3, FG1]	Sensitivity analysis of intralayer time-based metrics; nonlinear uncertainty in human layer
Systemic behavior and performance monitoring of both process and product will identify problems early	Time between detection and notification to the security alarm station [6]	Interlayer and intralayer distances between the nodes based on routes and bandwidth
	Network resilience to recover in the event of a disruption [2]	***Define system recovery in terms of interlayer bandwidth and communication availability rate***
	Redundancy of infrastructure (e.g., power, water) systems [6]	Intralayer edges (e.g., cascading failures from removing edges)

MLN approach invoking complexity/systems/network theories → helps address gaps in HCF security

MLN-based approaches helps address need to "integrate a system security science" (INCOSE)

MLN-base systems security engineering → move from "reactive" to "proactive" to mitigate complexity

QUESTIONS?