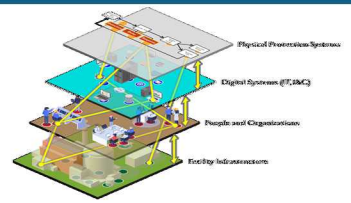
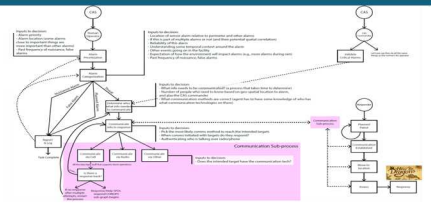
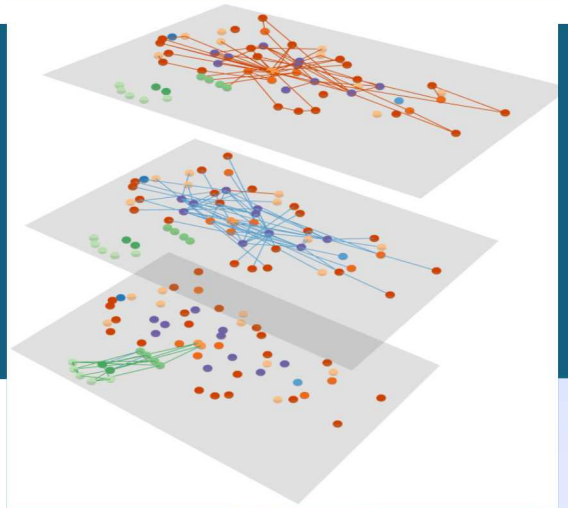
SAND2020-7284C

A Complex Systems Approach to Develop a Multilayer Network Model for High Consequence Facility Security







PRESENTED BY

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

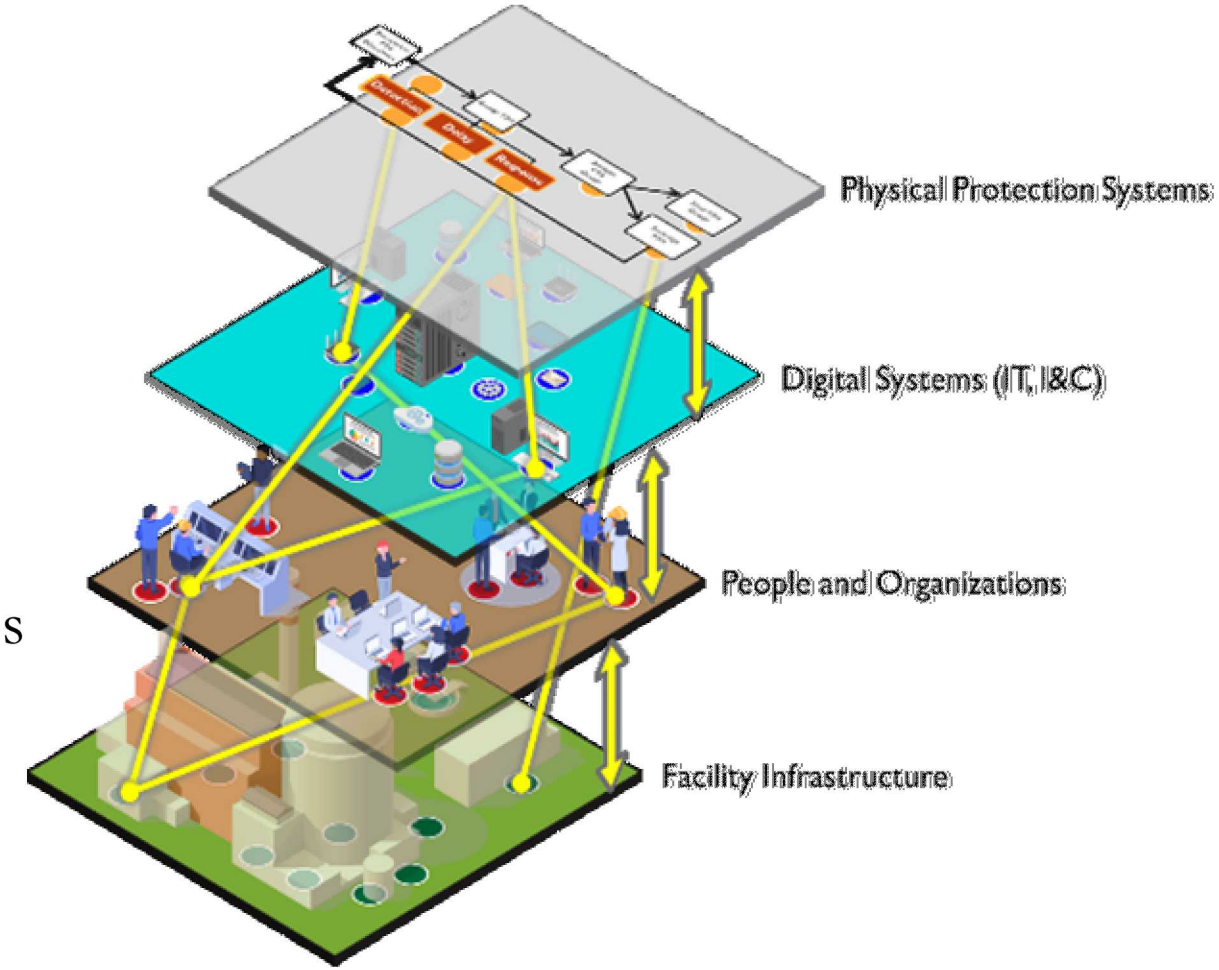
International Conference on Complex Systems

July 2020

SAND2020-TBD. 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
- Multidomain Interactions in HCF Security
- Multilayer Network Model for HCF Security
- Demonstration Case: HCF Security Scenarios
- Insights & Implications



Introduction

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

- Increasing/changing adversary capabilities (e.g., UAS, cyber attacks, insiders)
- Different operating/system conditions (e.g., increased digitization & interdependency)
- Reduced control over operational environments (e.g., remote locations or new geographical areas)

Result → challenge to efficacy of current security paradigms

Response → Current Sandia LDRD research hypothesizes

- Interactions matter!
- Multidomain interactions of HCF security can be modeled as a multiplex
- High consequence facility (HCF) security → complex system behavior

2019: Yemeni rebels use UAS to attack Saudi Oil facilities

2019: Cyber attack on Indian Kudamkulam Nuclear Power Plant

2011: DHS memo "violent extremists… insider positions"

LDRD

Multidomain Interactions in HCF Security

Data Collection

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

Data Analysis = Key insights + major themes

Theme 1: Current "siloed" nature of HCF security

- "stovepipes kill us" in HCF security → interactions matter

Theme 2: Inadequate accounting for role(s) of humans

- Best systems cannot overcome humans who ignore it!

Theme 3: Incomplete threat characterization

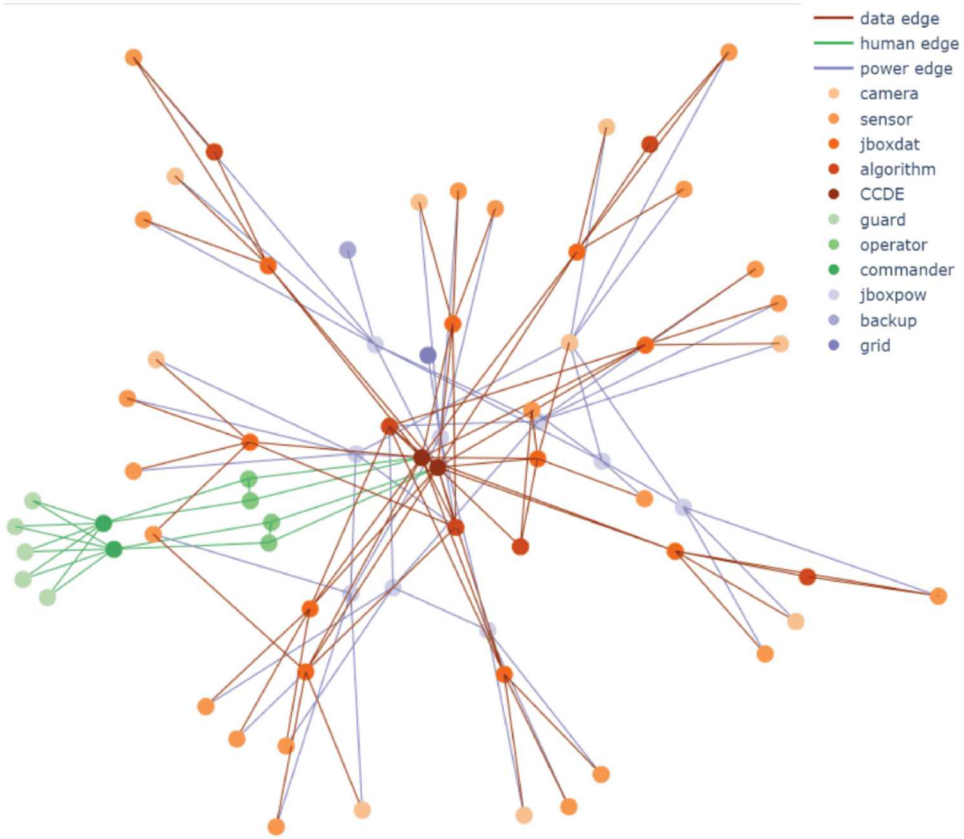
- Need to overcome "seeing is believing" mindset

Int.	HCF Security-Related Role	Training in Current HCF Approaches	Years in HCF Security-Related Role(s)*	Formal Analytic Background
A	1	Formal	>10	No
B	1	Formal	>10	No
C	2	Informal	>2	Yes
D	1	Informal	>10	No
E	3	--	>6	Yes
F	4	Formal	>2	Yes
G	5	Informal	>5	No
H	5	Formal	>10	No
I	3, 4	--	>5	Yes
J	4	--	>10	Yes
K	1	Formal	>20	No
L	5	--	>10	No
M	4, 6	Formal	>30	Yes
N	7	--	>10	Yes
O	4, 6	Informal	>30	No
P	3, 4	Formal	>15	Yes
Q	1, 4	Informal	>5	Yes
Focus Group 1	6	Informal	2 to 30+	Some
Focus Group 2	1, 5	Informal	0.5 to 7	No

1. HCF Security Engineering; 2. Cyber Security Analysis; 3. HCF Resilience Analysis; 4. HCF Security System Analysis; 5. HCF Security Technology Development; 6. HCF Security Operations; 7. Human Cognition in HCF Security

**This refers to cumulative years in HCF security-related roles, not just the current role*

Multilayer Network Model for HCF Security



Leverage key insights from:

- Complex systems theory → non-linear, parallel cause & effect
- Network science → define, measure, & priories node relationships
- Multilayer networks → multidimensional/domain interactions

Capture HCF security in terms of three layers:

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 command/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)

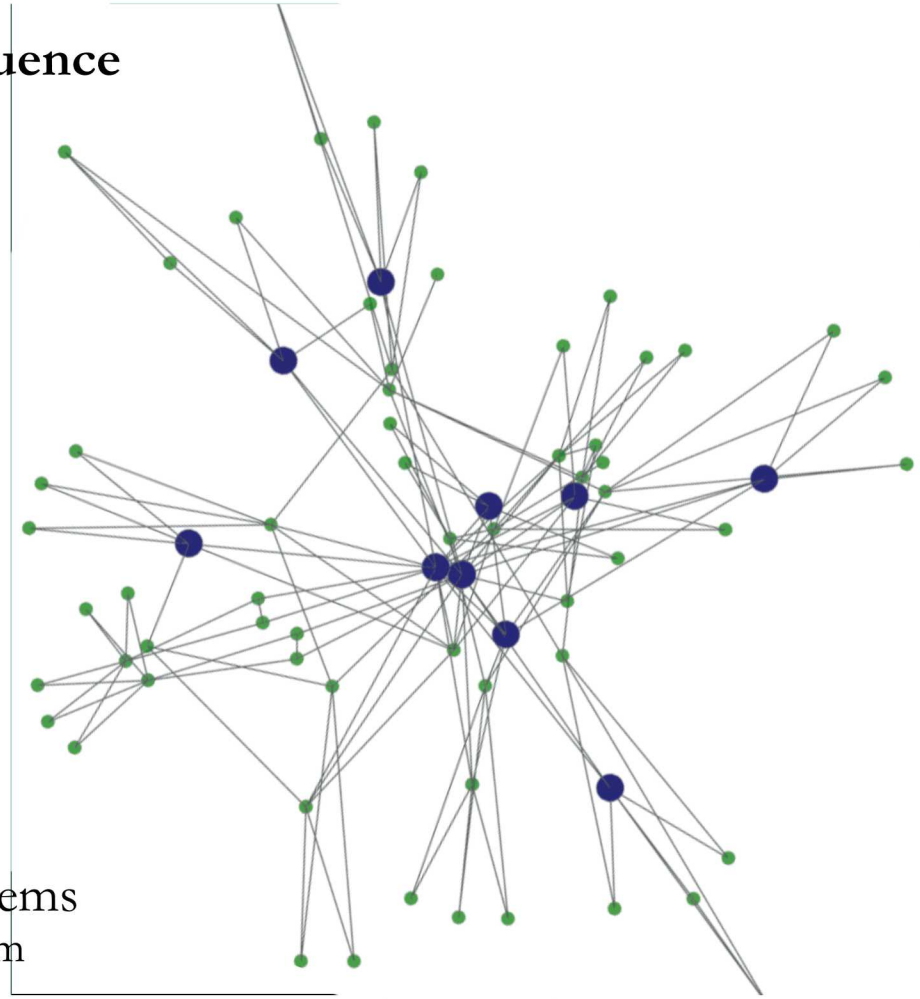
Demonstration Case: HCF Security Scenarios

Hypothetical High Consequence Facility (H2CF)

10 distinct perimeter intrusion detection systems

Each sector consists of
- Sensors devices
- Cameras
- Algorithmic processors
- Junction boxes
- Network switches

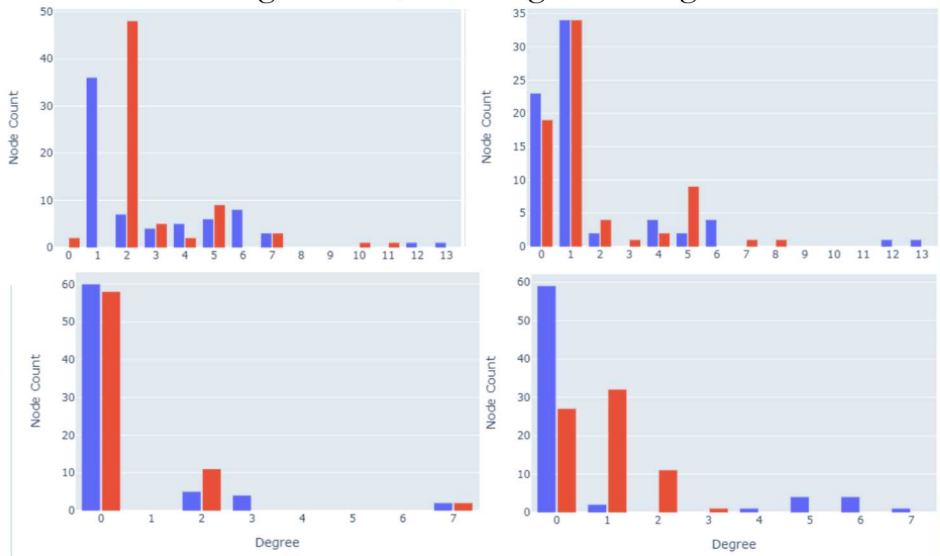
All data feeds to a central command/control/display systems
- Includes video management system
- Primary human interface



PageRank values for H2CF, with blue circles representing highest pagerank scores

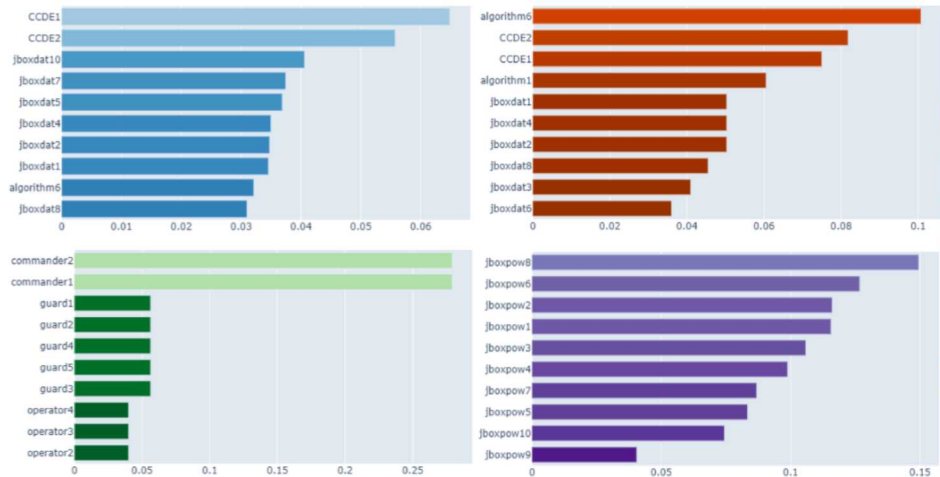
MLN "Flat" Model

Figure + In/Out Degree Histograms



MLN PageRank

Figure + Histograms



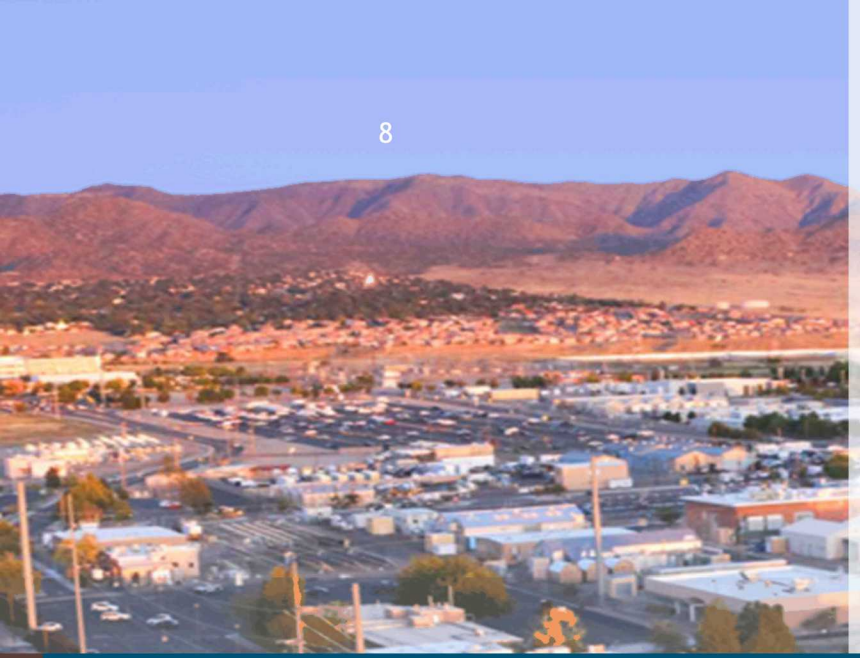
Insights & Implications

Key multilayer network-based insights:

- Large in-degree/low out-degree in power layer → highly centralized, directional, & dependent
- Large # high degree nodes + small # low degree nodes → potential power law relationships (hubs)
- Highest PageRank (flattened) = command/control systems (*intuitive*), junction boxes (*non-intuitive*)
- Highest PageRank (combined) = algorithmic switches (*non-intuitive*), command/control systems (*intuitive*)

Implications from successful demonstration of H2CF multilayered network model:

- Quantitative evidence of qualitative insights (e.g., importance of data aggregation elements—junction boxes)
- By extension, new design opportunities for resilience or optimized performance
- Data themes support expansion from prescriptive, "threat-based" to holistic, "threat-agnostic" HCF security
- Supports systems security transition from a static to a dynamic paradigm
- HCF security via ***interactions*** to counter real complexities, innovative adversaries, & disruptive technologies



QUESTIONS?