SAND2021-9312C

Early Results from Applying a Multilayered Network Framework to Engineer 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, Albuquerque, NM, USA, [adwilli; gcbirch; sacaske; eflemin; tgunda; thoadams; jwingo; jstverak] @sandia.gov*

Engineering nuclear security systems is a consistently challenging endeavor that requires sociotechnical solutions capable of addressing evolving and dynamic complexity. Next-generation engineering approaches for securing nuclear facilities and materials need to address challenges stemming from complex risk environments, innovative adversaries, and disruptive technologies. Leveraging key insights from the advances across several academic domains provide opportunities for incorporating systems security engineering to generate nuclear security solutions capable of addressing these sources of complexity.

Current research at Sandia National Laboratories hypothesizes a systems security engineering approach that describes nuclear security as a multidomain system visualized as multiple, interacting layers. From this perspective, security performance is a set of emergent behaviors from complex system interactions rather than traditional, highly linear security models. Building on the strong history of current approaches, this research re-examines core analytical assumptions for nuclear security to better incorporate interdependencies, dynamics, and n^{th}-order effects observed—and anticipated—in operational environments for nuclear security. The result is a multilayered network-based approach that captures the interactions between infrastructure, physical components, digital components, and humans in nuclear security systems.

* SAND2021-TBD. 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. Disclaimer: This paper describes objective technical results and analysis. Any subjective views or opinions expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government. This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

Key themes generated by a series of qualitative, semi-structured interviews (and several focus groups) from various high consequence security experts highlight the need for integrating complex system theory and resilience science in methodological assessments. This paper will discuss how these empirical insights were translated into a multilayered network framing, including a review of various multilayered network representations. This paper will then share example results from applying this approach to nuclear security—including novel outcomes. Lastly, this paper will discuss insights, implications, and the potential for future work in multilayered network-based approach for nuclear security.

Introduction

Engineering nuclear security systems is a consistently challenging endeavor that requires sociotechnical solutions capable of addressing evolving and dynamic complexity. Next-generation engineering approaches for securing nuclear facilities and materials need to address challenges stemming from complex risk environments, innovative adversaries, and disruptive technologies. Despite a strong history, classic security paradigms struggle to address the impacts of such increasing complexity on security performance. Relying on traditional performance measures like probability of detection, delay time, and response force time, related methodologies often (at best) simplify and (at worst) ignore complex interactions observed in real nuclear security system performance.

Leveraging insights from several academic domains helps incorporate systems security engineering into generating nuclear security solutions capable of addressing these sources of complexity. From this perspective, security is *not only* a microwave sensor alarming when an intruder is in the perimeter OR a steel reinforced wooden door at a sensitive facility OR an armed protective force deploying to a potential conflict situation—security *emerges* from the *interactions* between these elements and actions. This replaces highly linear models of nuclear security with a multidomain system visualized as multiple, interacting layers. The result is a multilayered network that captures the interactions between infrastructure, physical components, digital components, and humans in nuclear security systems.

Rather than continuing to sectorize security, this multilayered paradigm captures interdependencies between elements of nuclear security. Consider, for example, the evolution of security visualized in **Figure 1**. In Figure 1[a], different aspects of nuclear facilities related to security—namely the facility infrastructure, people (and organizations), digital systems, and the physical protection system (PPS)—are modeled *individually*. This is consistent with a common underlying premise of current security paradigms—that effective PPS performance is determined independently.

Yet, as interactions between these elements are observed in practice, then they should be included as comprehensively as possible. Consider, for example, the need for elements of underlying facility infrastructure to supply electrical power to intrusion detection sensors—which then rely on network cables and information processors to communicate alarms to security personnel. As shown in **Error! Reference source not found.**Figure 1[b], including these interactions can be illustrated as connections between previously assumed independent aspects of security. Leveraging characteristics of resilience, complexity, systems, and network theories, this perspective of security incorporates interactions across domains that result in multi-domain emergent properties. Figure 1[c] represents one possible outcome—a multilayer network (MLN) model of nuclear security that includes multi-domain interdependencies.

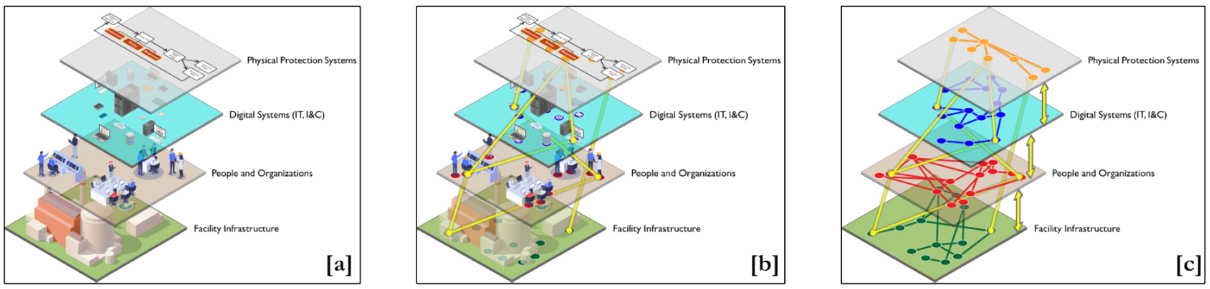

Figure 1. Models of nuclear security with [a] independent layers in traditional security paradigms; [b] connected layers in traditional security paradigm; and [c] connected layers in traditional security paradigm as a multilayer network model.

Key Themes from Empirical Data

Several key themes emerged from empirical data representing a range of perspectives on nuclear security that support the efficacy of using MLN models for nuclear security.

Though more details are provided in [1], this empirical data consisted of interviews and focus groups with nearly 30 experts across a range of nuclear security-related missions at Sandia National Laboratories. For data analysis, these experts were categorized using the concept of "worldviews" offered by the International Council on Systems Engineering (INCOSE) [2, 3]. These worldviews (summarized in Table 1)—or common models of nuclear security philosophy and practice—helped leverage key insights from experts across different areas of expertise to better address current nuclear security challenges. Using worldviews contributed to determining the robustness and validity of observed patterns and themes in the data.

Table 1. Summary of nuclear security "worldviews"

Nuclear Security World View	Description
Traditional Security	Experts involved in execution of DEPO—and DEPO-related—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.

Training and years of experience were also used to evaluate the generalizability of the patterns between worldviews and resulting themes, with an even split between worldviews (traditional security (7), emerging security (6), and systems analysis (7)), more early (1-9 years) and mid-career (10-19 years) experts than late career (20+ years) experts; and, an even distribution between formal and informal training backgrounds between the three worldviews.

Evaluating the empirical data—particularly investigating commonalities between worldviews relating to opportunities for moving toward ideal future states of nuclear security—identified several key themes. Similarities within the data and the spread of the data across worldviews suggest the trend analysis results and insights are more likely to be reliable, valid, and generalizable. Three key themes related to current and future states of HCF security were observed in the data: 1) changing operational designs and contexts, 2) methodological shortcomings, and 3) cultural influences. Each of the three themes were highlighted by experts from all three worldviews, with traditional security professionals being marginally more sensitive to changing operational designs and contexts than the other worldviews. Figure 2 shows a Sankey diagram—visualizations providing robust and easy-to-understand maps of relationships between key concepts [4]—to illustrate the relationships between these key themes for nuclear security and nuclear security worldviews.

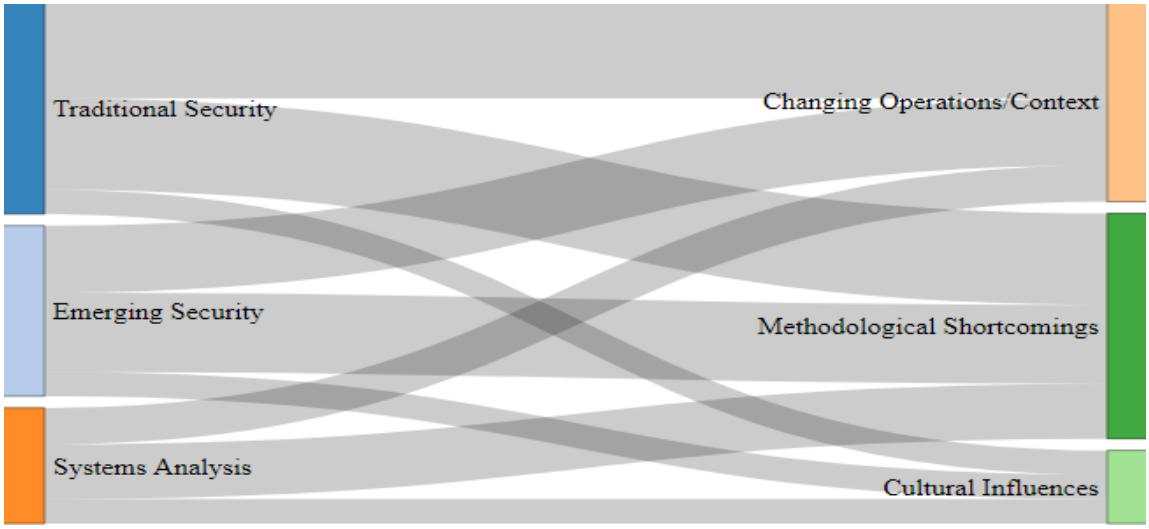

Figure 2. Sankey diagram of HCF worldviews vs. empirically derived common themes for the current state of HCF security (NOTE: Width of the bands indicate importance of theme)

The *changing operational designs and contexts* theme focused on spatiotemporal variations of nuclear security mitigations—including the effectiveness of past investments continue in meeting current performance needs, impact on operational security performance, and the transferability of nuclear security performance across different locations. In this theme, experts noted the changes in security operations (and

the environments in which security operations are expected to succeed) may be driven by maintenance concerns, differences in nuclear facilities/activities, training needs, and levels of monitoring for emerging threats. Related challenges arising from implementing current assessment approaches in locations where the local specifications did not match those often assumed in current security assessments were also identified by experts in this theme. Experts also described the how issues of complacency can often emerge with operators conducting routine tasks. Overall, the empirical data described how *changing operational designs and contexts* are a reality that influence both the current state of a security as well as associated assessment activities.

The *methodological shortcomings* theme concentrated on related to analytical approaches for conducting HCF security assessments. Oftentimes, this theme manifested as siloed nature of activities, incomplete threat categorization, and inadequate consideration of human (and organizational) factors within security-related analysis. Interestingly, patterns within this theme were more consistently identified by experts from all three worldviews. Consider empirical data highlighting the *siloed nature of security activities* (including assessments) as a significant issue. The data indicated that silos occur across almost all security-related activities, including limited interactions between protection force and facility operations personnel, between site design and site assessment personnel, and between different site security-related operations (e.g., cyber experts and physical site experts). The ramifications were pointedly described by one expert who stated that "stovepipes kill us because adversaries do not think in stovepipes." Again, the empirical data provided examples describing how *methodological shortcomings* manifest in challenges necessary to address for advancing the current state of nuclear security.

Finally, the *cultural influences* theme captured institutional and attitudinal factors that impact HCF security activities and observed performance. These data provided more insight into a wide range of "non-technical" and "social" factors that impact nuclear security operations and performance. Examples include institutional dynamics, formal and informal policies, and attitudinal influences on the state of security. Though observed in all worldviews, these *cultural influences* manifested as considerations for

policy issues by traditional security professionals and as risk attitudes by emerging security and systems analysis professionals. Cultural influences also manifest "on the ground," as various experts described how security analysts can become set in traditional modes and approaches, making it challenging to discuss—let alone include—cross-sector issues or observe unaddressed interdependencies. There is a clear connection between *cultural influences* and *changing operational designs and contexts* in nuclear security.

The collective impacts of the patterns evaluated in the experts' insights were incorporated into a force field diagram (FFD). FFDs are based on the concept of balancing how positive and negative forces influence overall system behaviors. More specifically, the role and relative influence of each force were captured from the data to describe how they either drove overall behavior relative to the ideal state or inhibited change [5]. Figure 4 visualizes the impact of empirically identified factors impacting nuclear security system performance elicited from thematic analysis. Each of the contextual factors in associated themes have an impact (either driving or inhibiting change) moving nuclear security towards a conceptual ideal state. For example, consider the prevalence of mentions in the data to the current siloed nature of security activities. This drift *toward* siloed security activities—commonly a byproduct of attempting some level of organizational efficiency—is a dynamic impact *away* from desired levels of performance (the "system design row in Figure 4).

Conversely, more actively monitoring emerging threats—which also increases a security system's adaptability—is a dynamic impact *toward* desired levels of nuclear security performance. Here, the extent to which nuclear security systems include proactive emergent threat monitoring (in contrast to more reactive threat updating schemas) the stronger the push toward desired levels of performance (the "monitoring" row in Figure 3).

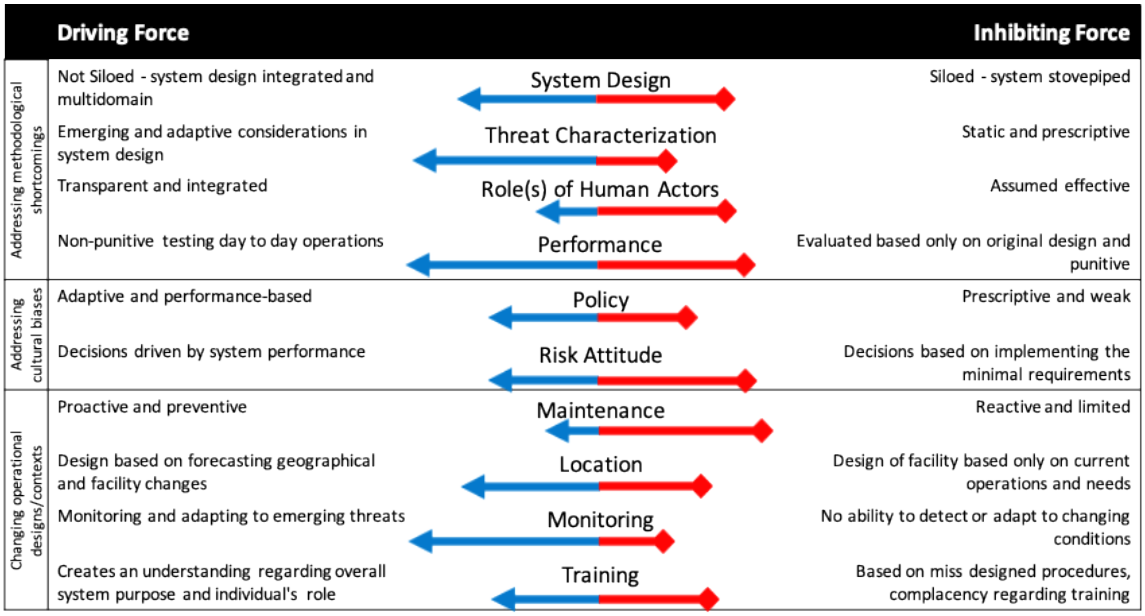

Figure 3. Force Field Diagram of factors influencing nuclear security, where arrow length indicates strength of impact. Blue arrows (R to L) are *driving towards* & red arrows (L to R) are *inhibiting against* the ideal security state)

These results suggest that using a systems theory-based paradigm for nuclear security will provide a strong foundation for improving gaps observed in the empirical data—including the specific mention of adopting a systems approach by almost all experts (17/20) across all three worldviews. Many of the insights from the FFD support the idea to conceptualize nuclear security as a multilayer network, where nodes represent key assets (e.g., cameras and guards) and edges representing different types of connectivity between nodes (e.g., data transmission). Such an innovative approach can directly leverage the analytical constructs and performance measures offered by the experts in the empirical data to improve the ability of systems and security assessments to reduce risks in nuclear security.

From Empirics to Multilayered Networks

These strong empirical foundations helped support an approach that represented these multidomain, but related, elements of nuclear security as a set of interacting networks. The multilayer network model of nuclear security systems is represented as both a

general multilayer network and as a multilayer network with explicit interlinks. The complexity of identifying and defining the multidomain interactions observed in nuclear security—and elicited from the empirical data—necessitated exploring various visualization techniques. Each have their own relative advantages, including (Figure 5):

- **Node Layer Representation** (Figure 4A) which generates simplified visual MLN models as a network of smaller connected networks distinguished by node type to more easily identify interlayer interactions;
- **Replica Node Representation** (Figure 4B) which visualizes all nodes on each layer but distinguishes each layer by node category which highlights elements of interdependence across node categories; and,
- **Aggregate Network Representation** (Figure 4C) which flattens the multiple layers into a single 2-D representation to aid in cognitive understanding and relating to more traditional network metrics.

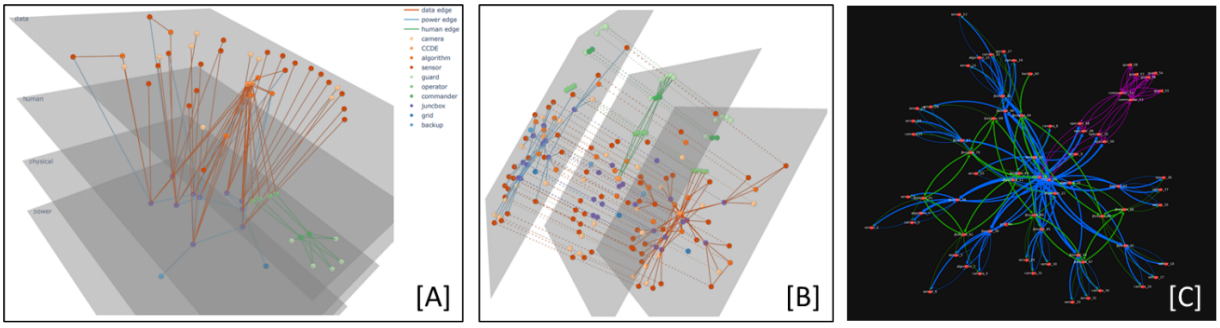

Figure 4. Example multilayer network model visualizations using [A] the node layer representation scheme, [B] the replica node representation scheme, and [C] the aggregate network representation scheme

As such, characteristics of these different multilayer network representations were incorporated into a new MLN-based approach for nuclear security. In addition, common single layer graph metrics are consistent with the themes emerging from the empirical data, including the roles of degree, connectivity, centrality, distance, transitivity and assortativity in describing nuclear security system behavior. Further, expanding into multilayer network metrics afforded the opportunity to explore how to communicate and evaluate the critical information contained in the edges connecting nodes in different

layers. For parsimony, consider two measures of multilayer network centrality, multilayer network page rank and eigenvector versatility [6]. *Multilayer network page rank* measures the centrality of a node in a specific layer, β, as influenced by the centrality of that same node in another layer, α. For nuclear security systems, this provides a mechanism for better representing the role of (often overlooked) junction boxes in overall performance. Similarly, *eigenvector versatility* of a node in a multilayer network is a measure of how much a node acts as a conduit for interaction between the layers of a network. This can help determine which nodes in the network are important transfer points between different connection types—or, in the case of nuclear security systems, important transfer points across security-related mitigations.

Similarly, a tailored simulation was developed to be extendable and flexible enough to represent holistic (e.g., multi-domain) nuclear security systems. Though working through different levels of simplification, the simulation was developed to incorporate data from different domains, particularly those that perform on vastly different timescales (e.g., from microseconds to minutes to hours) within the concept of "systems security." The code base draws heavily on object-oriented paradigms, particularly in an attempt to encapsulate particular data and behaviors into regions of data—termed "objects"—that can be treated as their own independent agents. Each object has control and access to its own internal state, allowing each to premise actions off knowledge of that state—thereby fully describing complex systems in terms of every characteristic each object uses to determine its current state. While some such events can be deterministically timed, most events are described as exponentially distributed random variables, which allows the entire operating state of the system to be modeled as into an extremely large Continuous Time Markov Chain (CTMC). This CMTC approach supports relatively fast Monte Carlo-style iterations and compressing evaluation events in spatiotemporal regions. These capabilities maximize flexibility within MLN model-based approach and better captures (and anticipates the behaviors of) multi-domain, different sized, and disparate time-domain layers.

Representative Multilayered Network Models Results

The success of early model development yielded interesting insights illustrating the ability of MLN models to support more advanced evaluations of nuclear security system performance across a suite of scenarios. For the following representative multilayered network model evaluation results, consider a 10-sector hypothetical nuclear security system consistent with international best practices for security design. Note that while this system still represents a simplified HCF security system primarily focused on perimeter intrusion detection system components, it consisted of 60 nodes and 216 edges between these nodes.

Various multilayer network metrics were explored considering this more detailed MLN model for a hypothetical nuclear security system. For example, Figure 5, below, illustrates a graphical representation [A] and bar chart [B] of the additive Page Rank metric—where node size and bar length are proportional to the centrality of nodes in one layer considering the centrality of that same node in other layers. Shown in both representations, the communication and control display equipment (CCDE) systems and alarm station commanders have the largest Page Rank value, with junction boxes also having higher comparative values within the network.

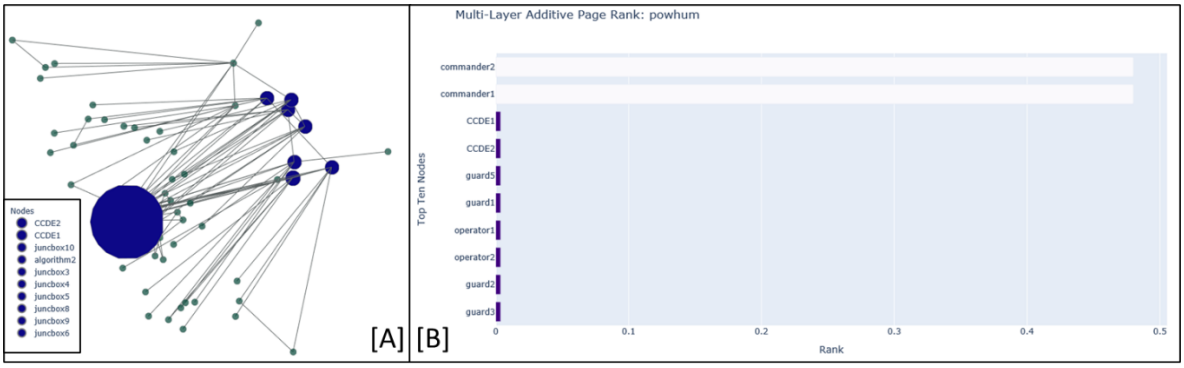

Figure 5. Graphical representation [A] and bar chart [B] of the additive Page Rank metric for a 10-sector hypothetical nuclear security system

One experiment was examined a "DEPO-like" metric—mean assessment time for alarms—with system architecture held static and only the probability of a false alarm increasing in subsequent Monte Carlo analyses. In addition to the generic parameters for the hypothetical nuclear security system described above, this simulation queried each

sensor every 10 time units to determine if it produces a false positive (FP) or true negative; FP rates range from 1%-10% (with the FP rate consistent across all sensors in a given simulation run), two security personnel assessed the alarms (with their assessment time ranging from 1 to 30 time units), and the newest alarm being assessed in the operator queue.

The results shown in Figure 6 are intriguing. Figure 6[A] illustrates the false positive rate of the sensors on the *x*-axis versus the operator assessment rate on the *y*-axis versus the mean assessment time on the *z*-axis. This analysis highlighted a region where mean assessment time is maximized in this system, as well as a prominent mean assessment time ridge where any single additional alarm results in a precipitous drop in mean assessment time in Figure 6[A]. Looking at the corresponding coordinate in Figure 6[B]—which shows the same values in the *x* and *y*-axis, with the *z*-axis displaying the total number of ignored alarms—this drop occurs alarms are building in the queue and are being ignored. The non-linear relationship between false positive rate and operator assessment rate demonstrated in this simulation highlights an interesting property of the "first in, first assessed" alarm assessment strategy—namely that after the mean assessment time ridge, if either operator assessment speed is slowed or sensor false positive rate is increased, alarms will begin to be ignored. These results not only match both intuition and observations, but they also represent a mathematical description that enhances nuclear security system analysis and design capabilities.

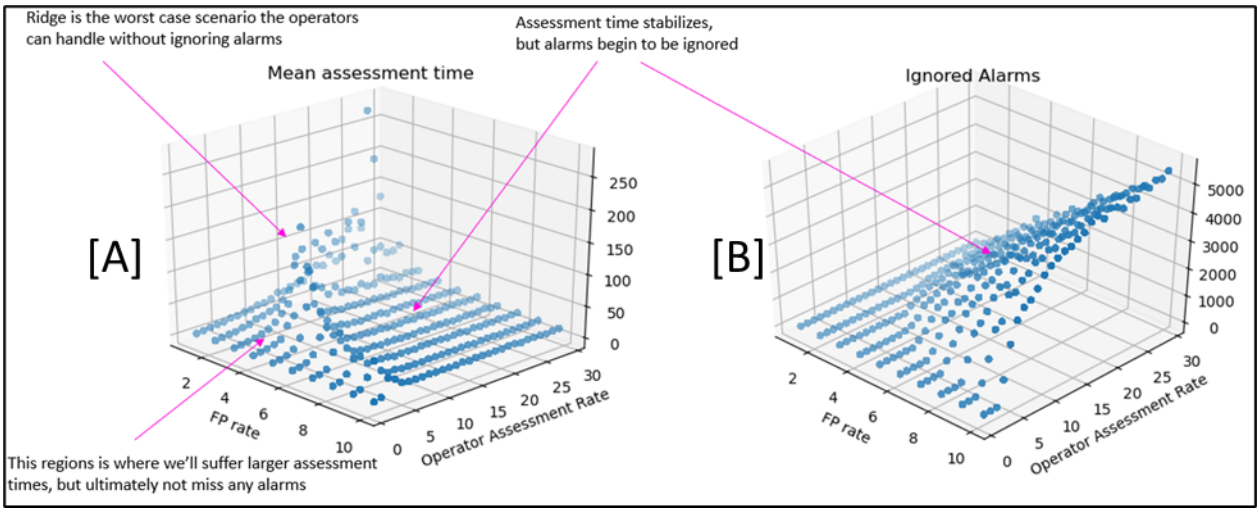

Figure 6. Results [A] mean assessment time and [B] number of ignored alarms as functions of false positive (FP) rate and operator assessment time for a 10-sector hypothetical nuclear security system using a "first in, first assessed" alarm assessment strategy.

An additional experiment investigated a more complex topological question to determine what percentage of removed edges in the nuclear security system MLN model would fail to report any sensor alarms. More specifically, this analysis investigated how randomly removing edges within the security system would ultimately impact information returning to the central alarm station. In addition to the generic parameters for the hypothetical nuclear security system described above, this simulation removed a random edge every 500 time steps until no data was reported. From a security perspective, it is worth noting that the "random" removal of edges could be thought of as cascading problems manifesting from accidental component failures (or misbehavior), intentional malfunctions, or a combination of the two. As shown in Figure 6, the results illustrate a non-linear relationship and a "tipping point" after which the security system cannot effectively function. This tipping point is directly tied to network topology. For example, in this particular 10-sector hypothetical nuclear security system, removing less than half the edges in the system results approximately 10% system operational functionality. From this perspective, the MLN topology of a nuclear security system is a critical consideration when evaluating the resiliency of proposed nuclear security system concepts and designs.

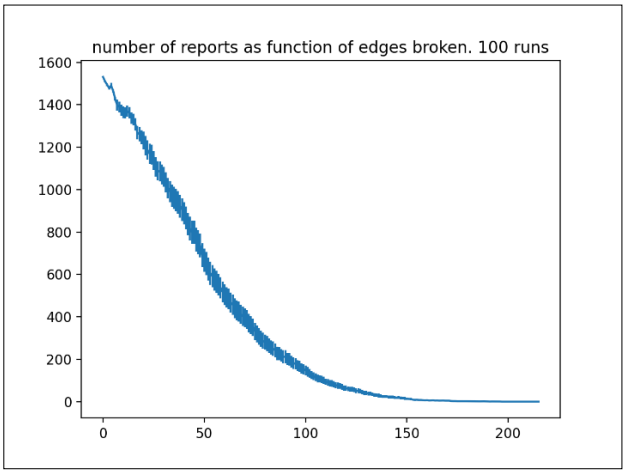

Figure 6. Results Monte Carlo-based topological analysis of random edge removal in a 10-sector hypothetical nuclear security system

Insights, Implications, & Future Work

These early results from investigating a multilayer network model-based approach for nuclear security show promise for keeping pace with the interdependencies, dynamics, and nth-order effects present in today's more complex operational environments. Accounting for cross-domain interactions in security seem necessary for a more comprehensive model of security that supports next-generation nuclear security systems. This research has extended thinking across disparate academic domains to initiate a transition from "reactive" to "proactive" security that could better align traditional security functions (detection, delay, and response) with real-world complexities.

The themes and insights elicited from the empirical data help describe potential opportunities to bridge challenges to and ideal future states of current nuclear security capabilities. In particular, the worldview-based data analysis helped identify commonalities between traditionally disparate perspectives of nuclear security that support a transition toward network-based performance measures for nuclear security behaviors. For example, complex system theory's emphasis on connections provides a mechanism for including the observed—but often overlooked—interactions between changing operational contexts and nuclear security system designs. Likewise, network theory's ability to identify (and quantify the impacts of) "key nodes" provides the structure by which to capture (and better explain) unexpected behaviors observed in nuclear security performance—like non-linearities mean assessment time and random edge removal.

These early results imply a viable path forward to better address both endogenous and exogenous challenges to current nuclear security paradigms. These include—but are not limited to—the role(s) of human actors, multidomain interactions, and non-linear operational environments, and anticipatory performance measures necessary to mitigate real-world complexities, innovative adversaries, and disruptive technologies. The multidisciplinarity, dynamism, and disparate time-scale synchronization inherent in

these multilayer models will help more holistically define, quantify, analyze, and optimize multidisciplinary security solutions.

REFERENCES

[1] T. Gunda, S. Caskey, A.D. Williams, G.C. Birch, “Revisiting Current Paradigms: Subject Matter Expert Views on High Consequence Facility Security Assessments,” *Journal of Nuclear Materials Management*, in-press, 2021.

[2] H. Sillitto, R. Griego, E. Arnold, D. Dori, J. Martin, D. Mckinney, P. Godfrey, D. Krob and S. Jackson, "What do we mean by “system”? - System Beliefs and Worldviews in the INCOSE Community," *INCOSE International Symposium*, vol. 28, no. 1, pp. 1190-1206, 2018.

[3] D. Rousseau and J. Billingham, "A Systematic Framework for Exploring Worldviews and Its Generalization as a Multi-Purpose Inquiry Framework," *Systems*, vol. 6, no. 27, 2018.

[4] P. Riehmann, M. Hanfler and B. Froehlich, "Interactive sankey diagrams," in *IEEE Symposium on Information Visualization - INFOVIS 2005*, IEEE, pp. 233-240, 2005.

[5] K. M. Adams, "Perspective 1 of the SoSE methodology: framing the system under study," *International Journal System of Systems Engineering*, vol. 2, no. 2/3, pp. 163-192, 2011.

[6] G. Bianconi, Multilayer networks: structure and function, Oxford university press, 2018.