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.

SAND2022-3517C

32nd Annual INCOSE
international symposium
hybrid event
Detroit, MI, USA
June 25 - 30, 2022

Multilayer Network Models for Coordinating Orchestration of Systems Security Engineering

Adam D. Williams
Sandia National Laboratories*
P.O. Box 5800
Albuquerque, NM 87185-1371
505-844-6779
adwilli@sandia.gov

Gabriel C. Birch
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-1006
505-844-1888
gcbirch@sandia.gov

Susan A. Caskey
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-1371
505-284-5095
sacaske@sandia.gov

Elizabeth S. Fleming
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0152
505-844-9135
eflemin@sandia.gov

Abstract. Systems security engineering (SSE) faces new internal (e.g., increased digitization) and external (e.g., adversary capabilities) obstacles as systems increase in complexity and are deployed to increasingly challenging operating environments. Legacy approaches heavily rely on individual, physical, digital, or personnel domain-specific strategies for security. Such segmented responses helped initiate efforts by the INCOSE systems security working group to identify fundamental elements of SSE. One of these fundamental elements is security orchestration, where the SSE goal is to coordinate between previously disparate security solutions. Multilayer network-based approaches seemingly provide the logical structure and mathematical foundation to conduct security orchestration for "tightly coupled coordinated system defense in cyber-relevant time." Within multilayer networks, the ability to identify and manipulate cross-domain (e.g., intralayer) connections that influence security performance measures demonstrates an enhanced level of security orchestration. As such, multilayer networks support the future of SSE efforts to mitigate real-world complexities, innovative adversaries, and disruptive technologies. After describing security orchestration as a concept and foundational element, this paper explores how multilayer network models can enhance orchestration systems security engineering. Additionally, a demonstration case of systems security for a high consequence facility (as a complex system) is followed insights and implications for incorporating orchestration in the future of systems security.

*Sandia National Laboratories is 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-NA-0003525. **SAND2021-PEER REVIEW.**

Introduction

Effectively securing systems against intentional or malicious disruption(s) in the future, according to Willett (2020), includes developing principles to capture non-linear, non-deterministic interactions between security systems and operating environments and incorporating context-inclusive methodologies for prioritizing security principles. Willett (2020) also asserts that

> Part of the challenge [in systems security engineering] is the lack of a system science discipline within which to integrate a system security science...Security is predominantly a heuristic practice where we encase that which works in some attempt at engineering for repeatability and consistency...[yet] developing the science of system security and security engineering is preferable over doing more of the same harder (heuristics). (Willet 2020, 5)

Systems security engineering faces new obstacles as systems increase in complexity and are deployed to increasingly challenging operating environments. Some obstacles relate to external influences, including advances in adversary capabilities, broader ranges of expected applicability, and reduced levels of control over operations. These external obstacles—particularly those relating to the adversary capabilities—traditionally receive dedicated protective measures. Consider personal computer operating system patches issued in anticipation/response to a demonstrated hacker capability, for example. Influences internal to complex systems can similarly challenge protective efforts. To the extent that complex systems have physical, digital, and personnel components, any update or modification of individual components can change system security effectiveness. Consider, for example, replacing analog control mechanisms with digital controllers. The structure of how these components are arranged within the system— including both technological and organizational architectures— influences system security. If legacy approaches protect physical, digital, and personnel components with individual, domain-specific strategies, then addressing related interactions is an often-overlooked obstacle.

In response, efforts to advance the state of systems security are more explicitly looking to account for and design for security emerging from individual component performance and the interactions between the performance of these components. Further, Dove and Willett (2020) argue that systems security engineering needs to incorporate a socio-cyber-physical paradigm that includes people, procedures, technologies, and environments. Explicitly addressing interactions to support a socio-cyber-physical paradigm necessitates approaches capable of capturing system behaviors across disparate time domains (consider microsecond decision-making in algorithms influencing physical positioning of sensors that may take minutes, for example). Rather than continuing to sectorize protective efforts, approaches are needed that help align and coordinate across traditional security domains—including physical, digital, and personnel security—to achieve desired levels of systems security. The resulting multi-domain security approaches should include the design and evaluation of the interactions within domains (e.g., ensuring sufficient cyber security architectures) and between disparate domains (e.g., ensuring coordination between digital controllers and physical processes). Such multi-domain approaches to security would support "dynamic security decisions in operations resulting in fast, relevant, and adaptable system defense" (Dove, et al. 2021). By extension, systems security performance would also be further enhanced with coordination with non-security elements in the broader facility or system.

Ultimately, transitioning from "reactive" to "proactive" security requires aligning traditional security functions with real-world complexities and coordinating across multi-domain interactions inherent within complex systems. One system security approach replaces highly linear, segmented models of systems security with a multi-domain model visualized as interacting layers. Leveraging insights from resilience science, complex system theory, and network theory, multilayer network models provide the logic structure higher-fidelity insight into emergent behaviors and expand the analytic solution space for systems security (Williams & Birch 2020). Further, empirical data from security professionals across the "traditional security," "emerging security," and systems analysis" worldviews (Sillitto, et al. 2018) corroborate the need for better understanding the multi-domain interactions observed in systems security (Williams, A.D. et al. 2021a).

Elements for advancing the state of systems security engineering in recent publications (Dove & Willett 2020; Dove & Willett 2021, for example) can be supported with multilayer network-based approaches. Consider the argument that agility in system security performance is necessary to contend with agility in adversary strategies and tactics. Empirical insights from (Williams, A.D. et al. 2021a) suggest that viewing security performance as system performance against current and new threats are related to measures of multilayer network centrality that describe how behaviors cascade. Similarly, if systems security engineering contends that interactions between human and non-human systems and processes need strategic attention, then (Williams, A.D. et al. 2021a) offers empirical support for using multilayer network performance measures based on intralayer edges between domain models. Lastly, empirical insights from (Williams, A.D. et al. 2021a) multilayer network performance measures such as interlayer bandwidth and communication availability rate describe the ability to recover from a disruption that supports calls for system behavior and performance monitoring to identify problems early in systems security engineering.

A multilayer network-based approach, however, is not a silver bullet solution for all thirteen fundamental elements for the future of systems security engineering (Dove, et al. 2021). Yet, based on the conceptual similarities provided in (Williams, A.D. et al. 2021a), a multilayer network-based solution can directly support several of these fundamental elements—most notable element no. 10, "security orchestration." The enhanced ability for multilayer network models for security to capture interactions (Williams, et al. 2021b) provides a capability for coordinating and orchestrating between the interactions. If security orchestration is important to the future of systems security engineering, there is a need to develop identification, design, and analysis mechanisms and methodologies.

Security Orchestration in the Future of Systems Security Engineering

As the needs for systems become increasingly complex, the art and science of designing engineered solutions that meet functional (and perceptual) requirements also increase. For any given engineered solution for a societal need, there exists some potential malicious or adversarial actions that could disrupt the related system from achieving its objective(s)—suggesting a need to better include protective elements into system design. Dove, et al. (2021) identified a set of postulated elements to serve as the foundation for incorporating system security engineering into INCOSE's "Future of Systems Engineering" (FuSE) initiative. Among such foundational elements as architectural agility, security as a functional requirement, and techno-social contracts is a common thread indicating the need for more coordination of needs, expectations, possibilities, and practical solutions in systems security engineering. More specifically, where complex systems consist of physical, digital, and personnel components, protective strategies are traditionally applied in terms of physical security, cyber security, and personnel security—with little, if any, regard for the interactions between them. In response, Dove, et al. (2021) offer security orchestration as a fundamental element of systems security engineering.

Table 1: Summary of trends for the future of systems security engineering, from (Willett, 2020).

Category	Architectural Premises for the Future of Systems Security Engineering
Foundational	• *integrate system security & cybersecurity engineering (mutually influential)* * • *context matters → context-aware systems with flexible human interfaces**
Strategic Framing	• security is an infinite game of continual adaptation to retain/regain the advantage • international coalitions for governance & adjudication to influence standards • avoid one-size-fits-all & create options with varying principles & risk tolerance • cybersecurity is (likely) the primary national security risk for many countries • *successful security & cybersecurity depend on successful national coordination** • hedge digital failures with analog alternatives → reduce risk in a digital world • *system value determines levels of resistance & resilience in the design** • avoid Gordian knots of liability by framing structure & accountability in design
Tactical Framing	• security is a functional requirement for engineered systems • the science of system security & security engineering is preferable to heuristics • *all technology is not equal & equality today's relationships may change** • adaptability ("to fix") & expendability ("to fry") are key to complex systems • compositional security, where readily available modules are less prone to error • *encoding axiomatic principles to facilitate non-deterministic systems action** • *automated logic in compositional security to resolve views across contexts*** • *design principles include varying (in)dependence in systems security*** • adaptively identify & encode early indicators as part of system design • context driven dependencies & constraints force prioritizing security principles

*Premises determined to influence the context for security orchestration
**Premises specifically identified by Willett (2020) for "security orchestration"

Simply stated, security orchestration is the foundational notion that traditionally applied disparate security solutions are least effective when operating individually and should seek enhanced coordination to improve performance. Yet, this coordination needs to be aligned with other trends related to advancing systems security. For example, Table 1 (above) summarizes the key fundamental premises for architecting the future of systems security engineering (Willett, 2020), including foundational premises and strategic premises that drive design and tactical premises that drive operational solution and implementation trade-offs.

The premises for systems security engineering Table 1 also provide additional context for adequately scoping potential security orchestration solutions. Willett (2020) focused on the idea that all complex systems moving forward that must be secured against external threats will have a significant cyber/digital contingent, a de facto argument to the increasing importance of coordination between protective strategies. Here, coordination presupposes an understanding of the interactions between "cyber security" and "system security,"—and orchestration presumes an ability to intentionally influence (either in design or operations) these interactions to enhance overall security performance. More specifically, Iyer (2019) defines security orchestration as

> connecting disparate security technologies through standardized and automatable workflows that enables security teams to effectively carry out incident response and security operations.

One attempt at modeling these interactions is addressed in another fundamental element of systems security engineering—techno-social contracts. As discussed by Dove and Willett (2021), techno-social contracts for systems security is an “approach to explicitly encode technology-to-technology rules of intra-protection and inter-protection as part of security orchestration.” While a good first step, this approach does not entirely address the lack of coordination across domain-specific security strategies.

Multilayer Networks for Enhancing Security Orchestration

However, multilayer network-based approaches for systems security engineering seemingly provide the logical structure and mathematical foundation to more completely capture these interactions and speak to the need for security orchestration that provides "tightly coupled coordinated system defense in cyber-relevant time" (Dove, et al. 2021). Multilayer network models capture these interdependencies as interactions within and between layers. More specifically, domain-specific security elements are included in individual layers, and any expected (or observed) interactions within elements in a single layer or between elements across layers are captured as edges between nodes in the network. Consider, for example, the evolution of systems security visualized in Figure 1. In Figure 1[a], domain-specific security elements—namely the facility infrastructure, people (and organizations), digital systems, and the physical protection system (PPS)—are modeled as interacting nodes within individual layers in a manner consistent with traditional approaches.

Yet, as interactions between elements in different layers are observed in practice, there is a need to include these edge connections across domain-specific layers (Figure 1[b]). Consider the need for facility infrastructure to supply electrical power to intrusion detection sensors, which rely on information processors to communicate alarms to security personnel. Translating these security elements into classic network nodes and edges—Figure 1[c]—provides the mathematical and logical structure to orchestrate the multi-domain interactions that drive emergent security behaviors with multilayer network models for systems security.

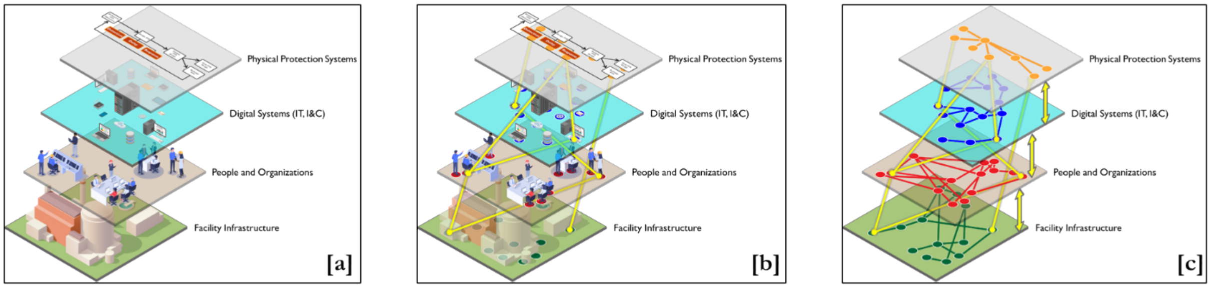
Physical Protection Systems
Digital Systems (IT, I&C)
People and Organizations
Facility Infrastructure
[a]
Physical Protection Systems
Digital Systems (IT, I&C)
People and Organizations
Facility Infrastructure
[b]
Physical Protection Systems
Digital Systems (IT, I&C)
People and Organizations
Facility Infrastructure
[c]

Figure 1. Models of systems 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.

The complexity of identifying and defining the multi-domain interactions observed in system security necessitated exploring various multilayer network visualization techniques. These various multilayer network perspectives provide different capabilities for describing security orchestration in these multi-domain interactions. Consider, for example, three different multilayer network visualizations. First, node layer representations generate simplified models as collections of smaller networks distinguished by node type to identify interlayer interactions easily. From this perspective, security orchestration focuses on connections between otherwise disparate layers.

In contrast, aggregate node representation flattens the multiple layers into a single two-dimensional model that aligns more easily to traditional cognitive understanding and traditional network metrics. Security orchestration focuses on interactions within a single network-layer from this perspective. Lastly, replica node representations visualize all nodes on each layer but distinguish each layer by node category, highlighting elements of interdependence across node categories. Here, security orchestration is achieved by coordinating inactions both within and between domain-specific layers.

Table 2: Mapping multilayer network models to how security orchestration fills gaps.

Gap	How Security Orchestration Fills Gap (from Iyer (2019))	Relevant Characteristics of Multilayer Network Models for Systems Security
A lot of data but little follow-up	*The security orchestration tool ingests data & performs actions based on predetermined actions*	• Provides structure to evaluate performance emerging from multi-domain interactions • Traditionally unused data can be captured into a suite of performance measures that capture emerging security behaviors
Tools that don't talk to each other	*Data from multiple products flows into security orchestration tool for centralized collection/ correlation of alerts*	• Structurally identifies & defines inflows/ outflows in terms of performance measures • A common (mental or systems) model to align domain-specific security solutions
People that don't talk to each other	*Playbooks provide codified best practices for analysts to follow, removing variation in response quality. Collaboration features provide structure and documentation support in real-time investigations*	• A common (mental or systems) model to coordinate discussions & decisions across security worldviews • Identifies & highlights focal areas to support real-time decision-making & investigations

Work to date on exploring multilayer network models for systems security have concluded efficacy and appropriateness for including non-uniform, multidomain interactions; evaluating dynamic performance metrics; and, incorporating widely disparate time scales between layers (Williams & Birch 2020; Williams, et al. 2021b). The success of multilayer network models to capture interdependencies and relational impacts between traditionally segregated domains of security strategies (e.g., physical, digital, personnel) indicate a clear role in the future of systems security engineering. The multidisciplinary, dynamism, and disparate time-scale synchronization inherent in these multilayer models directly support the fundamental need for improved coordination with systems security. Multilayer networks can provide more holistic security orchestration—including defining, quantifying, analyzing, and optimizing multi-domain solutions for systems security needs (Table 2).

Demonstrating Security Orchestration with Multilayer Networks: Lone Pine Nuclear Power Plant

As they can be considered complex systems (Williams, et al. 2021b), high consequence facilities provide a good demonstration case for security orchestration. For this example, consider the hypothetical Lone Pine Nuclear Power Plant (LPNPP)—a realistic nuclear power plant model that Sandia National Laboratories use for training and demonstration purposes. LPNPP facility operates continuously and consists of a pressurized water reactor, a primary coolant loop, a closed separate power conversion system, steam turbines, and several supporting buildings. The notional security system associated with LPNPP consists of detection (e.g., sensors, cameras, and monitors), delay (e.g., fences, reinforced doors, and vaults), and response (e.g., posted and patrolling guards) features commensurate with international best practices for protecting nuclear plants (Osborn, et al. 2019).

A combination of security and modeling subject matter expertise was used to transform this notional power plant into a multilayer network that included sensors, network components, power systems, communications lines, aggregating junction boxes, and other security elements. (For clarity, cybersecurity elements of LPNPP were simplified to help demonstrate the value of this approach.) The multilayer network model also captured the features of different edge types as multi-edge connections between nodes, with each edge representing relationships between data/communications, delivering power, or human interactions with a component. In general, edges are built using logic determined by common security system configurations—communication network configuration is expected to have sensors and cameras reporting to switches in junction boxes and on to centralized alarm stations, for example. This multilayer network model further serves as the foundation for a multi-agent simulation designed to operate with different components on different timescales, capturing unspecified behavior in activities that proceed through multiple domains and components. The result is an object-oriented, agent-based continuous time, discrete event-based simulation of multilayer network model performance.

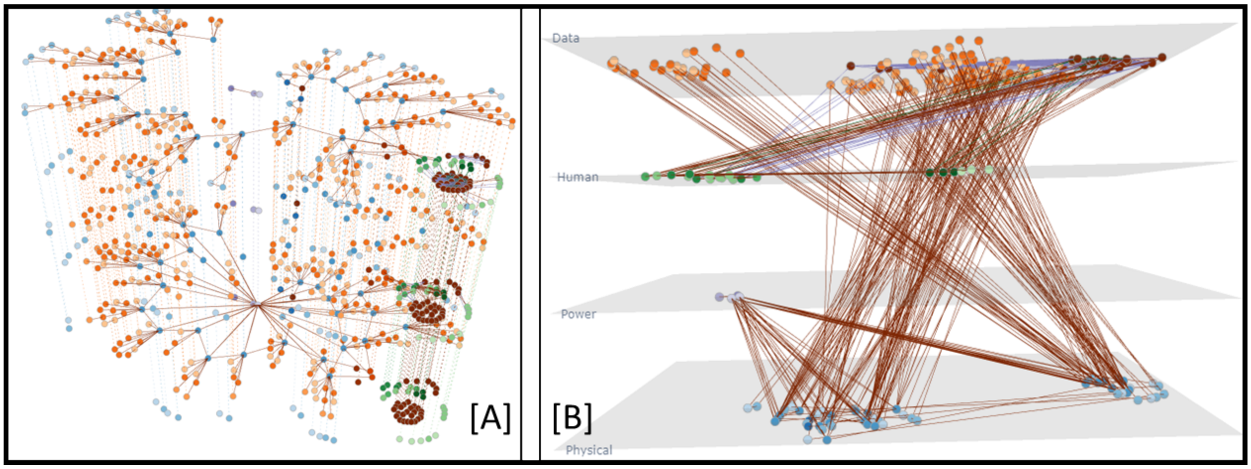

Figure 3. Multilayer network model visualizations for the hypothetical Lone Pine Nuclear Power Plant using [A] the replica node representation and [B] the node layer representation.

Consider how Figure 3 illustrates two different multilayer network model representations for LPNPP. Fig. 3[A] illustrates a replica node representation in which all nodes are included on all layers to help situate cross-domain interactions. In this representation, if a node on the power layer interacts with a node on the data layer, that connection is shown on both layers (either between the actual power node and a replica communications node on the power layer or vice versa). The resulting image of branches and clusters indicates coordinating and orchestrating between previously disparate security solutions. Similarly, Fig. 3[B] illustrates a node layer representation in which nodes are only captured in their respective layers, and cross-domain interactions are shown as intralayer edges. Here, security orchestration is illustrated as both the pattern(s) of intralayer edges (e.g., cross-domain interactions) and interlayer edges (e.g., in-domain interactions.

This multilayer network model and simulation for system security also provide opportunities to manipulate the system toward desired behaviors quantifiably—or, at worst, manipulate the system away from undesired behaviors. This approach also allows exploring how to communicate and evaluate the critical information contained in the edges connecting nodes in different layers, electrical power interacting with motion cameras, or personnel interacting with centralized alarm stations. More pointedly, consider the possibility for a failure to cascade through a complex system with undesired behaviors being passed both between system elements and across domains. Consider, for example, a compromised digital component that displays erroneous data to a human operator, who responds with physical changes that negatively impact security performance for the system.

A preliminary experiment to evaluate the ability of a multilayer network model of security system to respond to such a scenario consisted of over 60 Monte Carlo simulations measuring communication of vital information to centralized alarm stations as the security system continued to degrade. Using the LPNPP multilayer network model, edges were destroyed between two random powered devices every 1000 simulation time steps until the total number of communication signals dropped to near zero. From this perspective, the removal of each random edge was followed by logic hypothesized in security system operations. For example, breaking a power connection to a junction box would result in the cascading removal of data edges between sensors connected to the same junction box as sensors cannot send data without power. Table 2 summarizes several versions of this experiment.

Table 2: Mapping multilayer network models to how security orchestration fills gaps.

Plot in Fig. 4	Experimental Condition	Conclusions & Insights
Green	• Random node removal • No communications rerouting in the security system	• Complete communications failure follows power law behavior • Baseline for pushing curve up & right
Blue	• Random node removal • Small communications rerouting capability in the security system	• Complete communications failure follows power law behavior • Rerouting capabilities delays complete communications failure

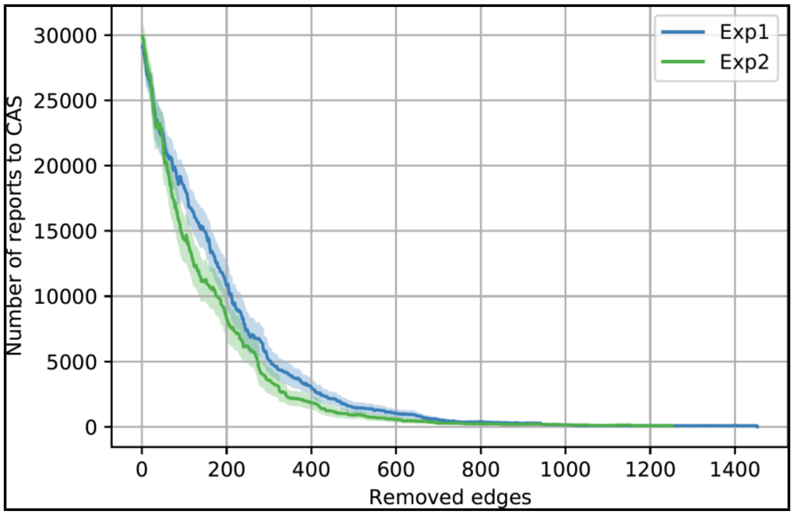

Figure 4. Number of reports sent to centralized alarm station as a function of removed edges, where solid line shows the average number of reports & the shaded region shows 90th percentile values, where the green plot represents a "no-brains" system and blue plot represents a "small brains" system with communication rerouting capability.

In a perfectly operating system, 100% of all communications would route to the centralized alarm station regardless of the number of broken edges in the multilayer network—notionally a horizontal line across the entirety of the simulation time at 30000 messages in Fig 4. While random edge removal assumes independence between security nodes not observed in practice, this experimental strategy offers simplicity and a baseline for understanding emergent security behaviors. In addition, all sensors produced signals at the same rate, enabling results to be interpreted as the proportion of sensors correctly communicating as a function of broken edges (Fig .4).

The levels of security performance illustrated in Fig. 4 provide an example output by which to orchestrate security solutions. This could include selecting specific elements or modifying connections between elements based on such characteristics as multilayer communicability—a centrality measure that quantifies the number of paths taking both intralinks and interlinks that join a given node of a given layer to the other nodes of the multilayer structure (Bianconi 2018)—to drive the system toward desired behaviors. Furthermore, the shape of the resulting non-linear reduction in communication effectiveness also speaks to the role that the topological structure of the multilayer network model has on emergent security behaviors. In other words, this indicates an opportunity to use topological decisions and structures to orchestrate desired behaviors among cross-domain security interactions.

Part of the elegance of multilayer network model-based approaches is the range of metrics that can be directly calculated (e.g., multilayer communicability from Bianconi 2018), as those that can be tailored for specific applications (e.g., Caskey, et. al 2021). For an example of the latter, consider two measures supporting the design principle of diversity. In system security engineering, diversity is a desired outcome to be orchestrated among selected components that exhibit significant variations to increase the difficulty of an adversary successfully manipulating system performance. One measure of diversity is the Shannon Index (also known as entropy score), which evaluates the proportional distribution of the difference of a particular type of component among all components supporting the same objective. For system security, consider the ratio of passive infrared sensors among the total number of different detection sensors. The other measure of diversity is functional redundancy or the level of (dis)similarity in the operational roles of system components. For security, consider how detection can be achieved by technical sensors, algorithmic pattern tracing, or human observation.

These two performance measures reflect structural (or topological) aspects of the security system that can be designed—and orchestrated. For the LPNPP, the measures used to define the Shannon Index and functional redundancy reflect the diversity in detection between line-based sensors, area-based sensors, and human observation. Similarly, communication diversity reflects the variance between the communication mechanisms (radio and hardwire), while assessment always relies on humans (alarm station operators or guards), so the defined variance is lower.

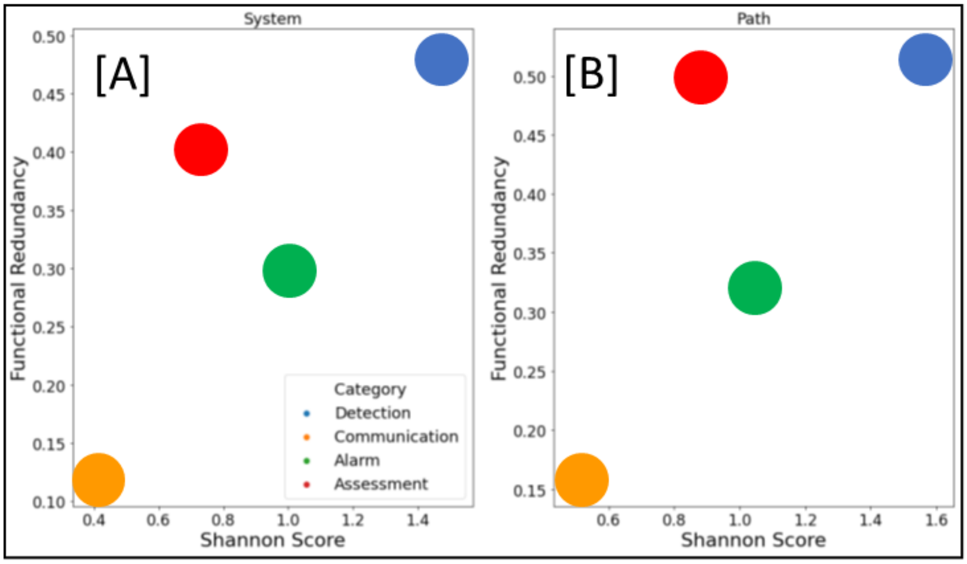

Figure 5. Summary diversity principle results for the hypothetical Lone Pine Nuclear Power Plant, plotting the performance measures Shannon Index versus functional redundancy, for the entire system [A] and along a representative adversary path [B].

Overall, the assessment capacity of the LPNPP (which has high functional redundancy but low Shannon Index values) highlights how multiple mechanisms to assess an alarm (monitoring video images or directly communicating with guards) can still offer limited variance in executing assessment. In this case, the attempts at diversity did not adequately orchestrate for both assessment techniques requiring human observation to determine the appropriate response. In a more orchestrated security system, both the Shannon Index and functional redundancy values would be higher and positioned in the upper right corner of Fig 5.

Insights and Implications

As demonstrated in visualizing and evaluating the multilayer network security model for the hypothetical Lone Pine Nuclear Power Plant, this approach provides multifaceted options for security orchestration. First, multilayer network model representations illustrate how security orchestration can be improved with a common, shared model of how and where interactions exist that impact desired (emergent) security behaviors. The cascading failure experiments extend this logic to illustrate how multilayer networks calculate the cross-domain influences on security performance. Lastly, the discussion on diversity performance measures demonstrates how multilayer network metrics directly support the ability to orchestrate desired security behaviors by manipulating the topology, including component selection and relationship definition. Table 4, below provides additional insights into how multilayer network systems' security models align with key premises related to security orchestration (Willett, 2020).

Table 4: Mapping elements of multilayer network models for system security to aarchitectural premises for the future of systems security engineering (Willett, 2020). (NOTE: the first two columns link to Table 1.)

Category	Premises for Future Systems Security Engineering: Security Orchestration	Related Elements of Multilayer Network Models for Systems Security
Foundational	• *integrate system security & cybersecurity engineering (mutually influential)*	• Common (mental/systems) model & cross-domain (intra-layer) measures
	• *context matters* → *context-aware systems with flexible human interfaces*	• Dynamic & topological multilayer network performance measures
Strategic Framing	• *successful security & cybersecurity depend on successful national coordination*	• Common (mental or systems) model of security & cross-domain (e.g., intra-layer) performance measures
	• *system value determines levels of resistance & resilience in the design*	• Dynamic/topological multilayer metrics → emergent behaviors
Tactical Framing	• *all technology is not equal & equality today's relationships may change*	• Dynamic & topological multilayer network performance measures
	• *encoding axiomatic principles to facilitate non-deterministic systems action*	• Emergent behaviors via component selection & relationship definition
	• *automated logic in compositional security to resolve views across contexts**	• Inter-/Intra-layer edge connections & related performance measures

	• *design principles include varying (in)dependence in systems security**	• Cross-domain (e.g., intra-layer) performance measures
*Premises specifically identified by Willett (2020) for “security orchestration”		

Within multilayer networks, the ability to identify the cross-domain (e.g., intralayer) connections that influence security performance measures demonstrates an enhanced level of security coordination; the ability to optimize these connections demonstrates an enhanced level of security orchestration. This paper demonstrated how using multilayer network models for security orchestration helps manage the complexity of security elements at a hypothetical nuclear power plant. By extension, this approach is anticipated to show similar success in capturing the additional complexity from incorporating more detailed cybersecurity features. While including cybersecurity features may significantly increase the nodes and edges needed to visualize the system, this multilayer network model is a good basis for insightful quantitative analysis.

As demonstrated, multilayer network models provide a viable path for security orchestration that better addresses more difficult cross-domain interactions—including human actors' role(s), dynamically evolving cyber security challenges, and non-linear operational environments. Maturity and deployment of such models will help develop security orchestration from a fundamental element to a security design mainstay. Multilayer network models also afford opportunities to orchestrate anticipatory performance measures to better mitigate real-world complexities, innovative adversaries, and disruptive technologies to enhance the future of systems security engineering.

References

Bianconi, G. 2018, *Multilayer networks: structure and function*, Oxford University Press, United Kingdom.

Caskey, S.A. et al. 2021, Leveraging Resilience Metrics to Support Security System Analysis, *IEEE International Symposium on Technologies for Homeland Security*, 1-7.

Dove, R. et al 2021, Security in the Future of Systems Engineering (FuSE), a Roadmap of Foundation Concepts, *INCOSE International Symposium* 31.

Dove, R and K. D. Willett 2020, 'Contextually Aware Agile-Security in the Future of Systems Engineering,' *IEEE/NDIA/INCOSE Systems Security Symposium (SSS)*, Crystal City, VA, USA, April.

Dove, R. and K.D. Willett 2021, Techno-Social Contracts for Security Orchestration in the Future of Systems Engineering, *INCOSE International Symposium* 30.

Iyer, A 2019, Security Orchestration for Dummies, John Wiley & Sons. <https://virtualizationandstorage.files.wordpress.com/2019/04/security-orchestration-for-dummies-demisto-special-edition.pdf>.

Osborn, D. M. et al. 2019, Modeling for Existing Nuclear Power Plant Security Regime, *Sandia National Laboratories, SAND2019-12014*.

Sillitto, H. et al. 2018, What do we mean by "system"? - System Beliefs and Worldviews in the INCOSE Community, *INCOSE International Symposium* 28 (1), 1190-1206.

Willett, K.D. 2020, Toward Architecting the Future of System Security, *INCOSE International Symposium* 30, 201-210.

Williams, A.D. and G.C. Birch 2020, A Multiplex Complex Systems Model for Engineering Security Systems, *IEEE/NDIA/INCOSE Systems Security Symposium (SSS)*, Crystal City, VA, USA, April.

Williams, A.D. et al. 2021a, Insights for Systems Security Engineering from Multilayer Network Models, *INCOSE International Symposium* 31.

Williams, A.D. et al. 2021b, A Complex Systems Approach to Develop a Multilayer Network Model for High Consequence Facility Security, Eds. D. Braha, M. de Aguiar, C. Gershenson, A Morales, L. Kaufman, E. Naumova, A. Minai, Y. Bar-Yam. *Unifying Themes in Complex Systems X (Proceedings of the International Conference on Complex System)*, Springer, 321-334.

Biography

Adam D. Williams is a Principal R&D System Engineer in the Center for Global Security and Cooperation at Sandia National Laboratories and serves as PI for multiple nuclear security projects for the National Nuclear Security Administration (NNSA) and Department of State. Dr .Williams is also a systems-theoretic analysis expert supporting projects in managing complex risk, system dynamics, physical protection system development and analysis, and global engagement.

Gabriel C. Birch is a Principal Electrical Engineering in the Autonomy and Unmanned Systems Group at Sandia National Laboratories. He has a Ph.D. in optical science from the University of Arizona College of Optical Sciences and his work at Sandia has focused on multi-disciplinary research into physical security systems and next-generation security concepts. Dr. Birch's area of expertise include physical security modeling, counter autonomy, and machine learning applied to physical security.

Susan A. Caskey is a Principal Member of the Technical Staff in the Global Security Research & Analysis Program at Sandia National Laboratories. Sue has more than 20 year's international security expertise and currently serve as the project lead for the analytical projects focusing on threat prioritization models and risk assessment models and tools. Mrs. Caskey has degrees in Biology, Computer Science, and an ME in Systems Engineering from Old Dominion University (ODU).

Elizabeth "Scottie-Beth" Fleming is a Senior Member of Technical Staff in the Human Factors Department at Sandia National Laboratories. Her work at Sandia uses a systems-based approach to analyze and improve human performance within complex systems. Dr .Fleming has applied human factors methodologies to a range of domains, including aerospace systems, nuclear power plants, energy grid, and physical security. She completed her Ph.D. at the Georgia Institute of Technology in Aerospace Engineering.