SAND2020-1096C

A Multiplex Complex Systems Model for Engineering Security Systems

1st Adam D. Williams
Center for Global Security and Cooperation
Sandia National Laboratory
Albuquerque, United States
adwilli@sandia.gov

2nd Gabriel C. Birch
Weapons and Force Protection Center
Sandia National Laboratory
Albuquerque, United States
gcbirch@sandia.gov

***Abstract*—Existing security models are highly linear and fail to capture the rich interactions that occur across security technology, infrastructure, cybersecurity, and human/organizational components. In this work, we will leverage insights from resilience science, complex system theory, and network theory to develop a next-generation security model based on these interactions to address challenges in complex, nonlinear risk environments and against innovative and disruptive technologies. Developing such a model is a key step forward toward a dynamic security paradigm (e.g., shifting from detection to anticipation) and establishing the foundation for designing next-generation physical security systems against evolving threats in uncontrolled or contested operational environments.**

***Index Terms*—security; complex systems; multiplex; interactions; emergence**

I. Introduction

Several dynamic trends are increasing the complexity in today's operational environment, which poses additional challenges to adequately providing security for high consequence facilities. One such trend relates to the pace of change in the threat domain, where demonstrated adversary capabilities include the use of unmanned aerial systems (UAS) and social engineering to move adversarial goals beyond traditional concepts of theft/sabotage (e.g., mass casualties at 2015 Paris attacks) [1]. A second trend relates to calls to more formally account for socio-technical interactions in high consequence facility security systems, especially when considering different observed system behavior when human decision making is replaced by artificial intelligence [2]. A similar trend stems from efforts to better understand how adaptable implemented physical security systems are to increasingly frequent changes in their operational environment [3]. Lastly, the increased digitization within controls of both operations and security systems at high consequence facilities significantly compresses the time in which security systems can achieve their protection goals [4].

These trends are challenging the efficacy and effectiveness of current security analysis paradigms based on assumptions of environmental control for high-consequence targets. For example, consider UASs. If used as an adversary tool (as demonstrated by the September 2019 attacks on strategic oil facilities in Saudi Arabia [5]), they directly challenge the usefulness of traditional detection measures as common ground-based prevention and detection mechanisms are insufficient in this scenario. If used by the facility itself, UASs can represent a force multiplier to expand protection capabilities beyond traditional security systems. Because existing security models are highly linear, they often fail to capture the rich set of interactions necessary to engineer security against 21st century threats.

In response, this paper introduces a new multiplex model for security of high consequence facilities. More specifically, this multiplex model describes security performance in terms of behaviors that emerge when multidomain physical security systems, the facility infrastructure, cybersecurity architectures, and human/organizational actor layers interact. After summarizing the current context of—and challenges facing—high consequence facility security, this paper incorporates insights from resilience science, complex system theory, and network theory as the foundation for a new security model. This paper then describes core elements of a multiplex model for system security, presents a representative use case, and offers implications and conclusions for engineering secure and resilient complex systems.

II. New Insights: Interactions Matter In Security

A. Current Context

One of the most cited methodologies for designing and assessing security at high consequence facilities is the Design Evaluation and Process Outline (DEPO) [6] created at Sandia National Laboratories (SNL). Invoking generic systems engineering concepts (e.g., feedback processes), DEPO borrows the underlying philosophy of probabilistic risk assessment-based approaches from nuclear safety. More specifically, accident timelines are replaced by two competing timelines: one for the required adversary action to achieve a malicious act and the other for response force actions necessary to protect high consequence facilities.

DEPO evaluates security as probabilistic influences on these timelines by calculating the ability of an arranged collection

SAND2020-XXXX. 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-NA0003525.

of security components to achieve a defined probability of defeating a specific adversary along a specific attack path. DEPO uses the detect, delay, respond paradigm to fully describe the necessary functions of a strong security design and evaluation framework [6]. As such, security performance is defined in terms of system effectiveness, which is represented as the product of the probability of interruption (e.g., the conditional probability that detection and delay system components will assess an adversary in time for response forces to arrive onsite to engage) and the probability of neutralization (e.g., the conditional probability that, upon arriving, response force capabilities can kill, capture or cause the adversary to flee).

Building on this legacy, subsequent efforts have evaluated thinking on the evolution of "next generation" security. Specific efforts include the evaluation of the role of risk complexity in nuclear security [7] and attempts to expand traditional paradigms by applying novel, systems-theoretic approaches to security of high consequence facilities [8]. Yet, there is still a need to more thoroughly address how future security systems can fully leverage the rich data present within a security system [9]. Another set of advances stem from applying resilience concepts and practices to explore and improve systems security, as demonstrated in the use of empirical data analysis to more effectively model preventive security maintenance decisions.

B. Challenges/Needs

The combination of increasing multidomain interactions required for securing high consequence facilities (e.g., increasing systems complexity) and demonstrated by evolving adversary capabilities (e.g., reduced controllability of operational environments) seems to necessitate a re-examination of core assumptions of security analysis. In addition, such a re-examination could also be used to develop a new paradigm to keep pace with the inter-dependencies, dynamics, and higher order effects present in today's more complex operational environment. Despite a strong history, current detect/delay/respond (DDR)-based security assessment methodologies (e.g., DEPO) struggle to account for this reduced control of operational environments. These methodologies simplify complex interactions and inter-dependencies observed in real physical security systems. From this perspective, security is not only a microwave sensor alarming when an intruder is in the perimeter, a central alarm station operator assessing an alarm and alerting the response force for deployment, or a firewall stopping malware attacks on sensitive information. Rather, *system security* emerges from the interactions between these actions.

As such, there is a need to explore the argument that interactions are necessary to better describe a more comprehensive model of security. Whereas advances are being made related to understanding interactions, they are occurring in disparate academic domains (e.g., resilience, complexity, systems, and network theories) and are tailored to fairly narrow phenomena of interest (e.g., resilient cyber systems). One response would seek to coordinate the rich insights from these disparate academic disciplines to build a more comprehensive model of security that includes multi-domain inter-dependencies. Such an approach has the potential to shift security from static to dynamic functional goals and from component-level DDR to system-level emergent security performance. Ultimately, this transition from "reactive" to "proactive" security would overcome the shortcomings observed in the current security analysis paradigm, align traditional security functions with real-world complexities, and incorporate the importance of multi-domain interactions into high consequence facility security.

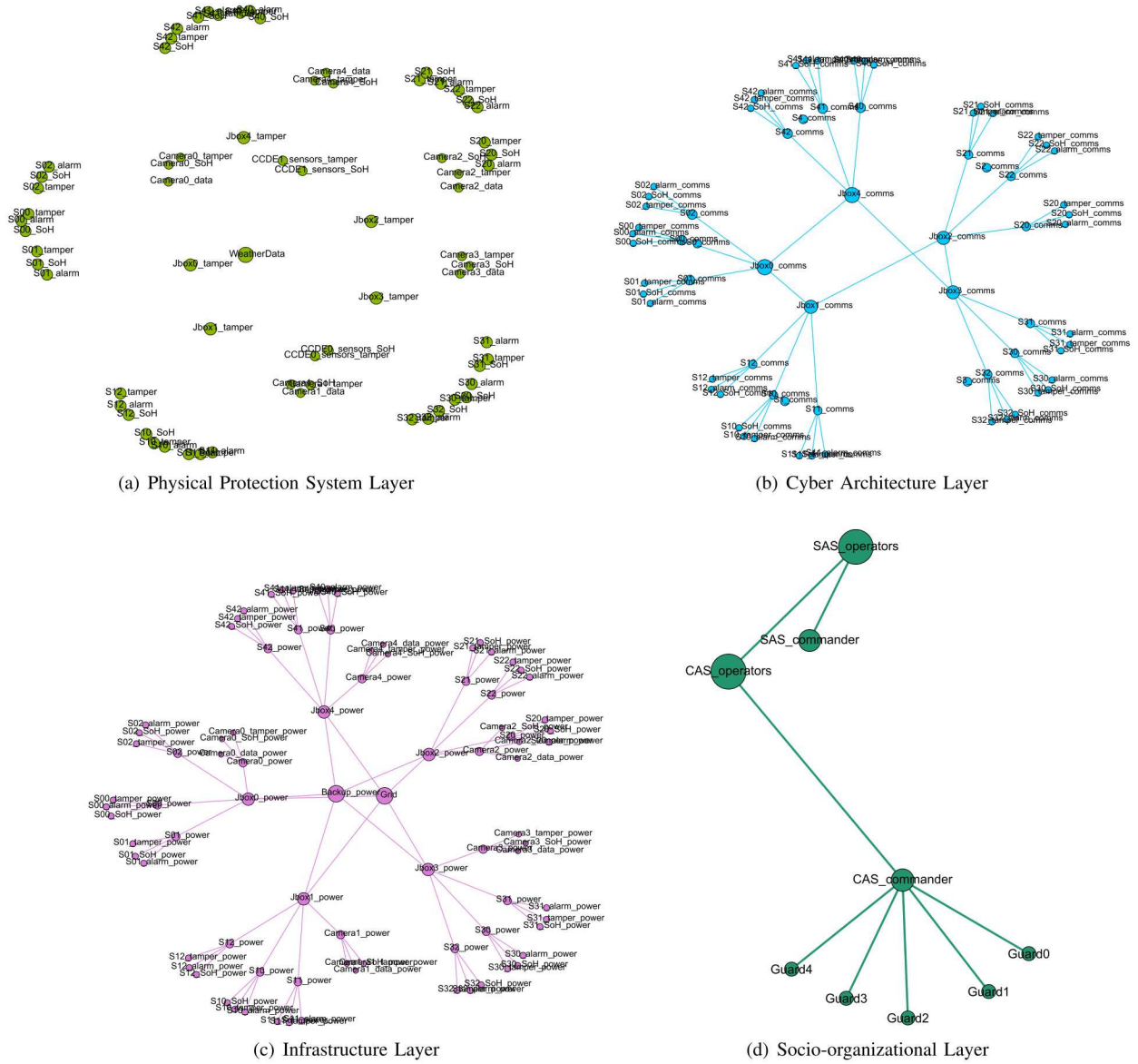
III. Multiplex Model Construction

A. New First Principles

Core concepts and recent advances in resilience, complexity, systems, and network theories offer insights to help organize these characteristics of next-generation security "first principles." First, resilience theory describes the capability and ability of a system or element to return to a stable state after a disruption [11]. This logic has been applied to describe mission execution despite an hostile cyber-threat environment and to evaluate how well energy systems prepare for, adapt to, and recover from disruptions [12]. In addition, the resilience theory performance measures of total recovery effort and system impact of disruption [13] [14] conceptually relate to high consequence facility security capacity and effectiveness, respectively.

Second, complexity theory "attempts to reconcile the unpredictability of non-linear dynamic systems with a sense of underlying order," [15] while systems theory was developed to address organized complexity [16] by providing a non-statistical, non-random logic to describe the behaviors of "many, but not infinitely many" [17] components. Further, the laws of physics [17] and sociology [18] argue that such systems naturally migrate toward states of greater disorder unless there are counteracting forces to maintain desired system behaviors. Complex adaptive system approaches also addresses how the specification of behaviors of many simple, interacting components can yield large-scale results that are more resilient to major environmental changes than the results of individual components would suggest. It is largely assumed that the cause of these results lies in the interaction of the agents which, despite lack of global knowledge, can still respond to large-scale changes [19]. Additional studies have demonstrated how complex adaptive systems approaches have performed automated search-and-retrieval with variable numbers of modular, cheap robotic agents robustly searching different target distributions [20]. This paradigm is also being used to develop a new model for detecting and responding to disease outbreaks based on principles of locality and scaling [21]. The results seen in these applications seem uniquely positioned to help address current issues with security approaches for high consequence facilities.

Lastly, network theory describes how relationships (or, interactions) characterize relative priority between nodes (or, system components) and describe emergent behaviors [22].



(a) Physical Protection System Layer

(b) Cyber Architecture Layer

(c) Infrastructure Layer

(d) Socio-organizational Layer

Fig. 1. Graph representation of in-layer connections of the four primary layers within the proposed multiplex model of physical security elements: (a) the physical protection system layer, (b) the cyber architecture layer, (c) the infrastructure layer, and (d) the socio-organizational layer. The example systems represented by these graphs describe an example perimeter intrusion detection security system.

Promising research applies concepts from network analysis to control of complex systems [23] and some aspects of high consequence security [24]. In addition, recent work has described, measured, and evaluated the behaviors of multiple interaction layers [25] [26] [27] [28]. Such systems are called multiplexes, and provide a visualization of how components within and across layers can interact. Coordinating the rich insights from these disparate academic disciplines provides the opportunity to describe the multi-domain inter-dependencies necessary to align next-generation security capabilities with current dynamic trends.

Leveraging these insights from the resilience science, complex system theory, and network theory domains can help overcome the challenges to the effectiveness and efficacy of current approaches for high consequence facility security. These new principles must not only account for what is in the security system, but how these elements interact with each other. For example, the interactions between different adversary mitigation mechanisms (e.g., physical security systems or cybersecurity architectures) are just at important as the performance of the individual adversary mitigation mechanisms themselves. More specifically, these first principles should explicitly account for the inter-dependencies observed between physical protection systems, the facility infrastructure, cybersecurity architectures, and human/organizational actors. Another characteristic to consider is the need for physical security systems to be adaptable to changes in demonstrated adversary capabilities and the controllability of its operational

environment. Similarly, performance of physical security systems should also be related to resilience, where the ability of the facility to maintain normal operations is achieved by either preventing or recovering from successful adversary actions.

B. Multiplex Model Conceptual Construction

Because multiplexes capture interactions within and between layers of interconnected components, they present a unique opportunity to model the multiple domains necessary to adequately secure high consequence facilities. The multiplex approach to security proposed in this paper incorporates a physical protection layer composed of sensing devices; a cyber architecture layer composed of digital components; an infrastructure layer composed of physical components; and, a socio-organizational layer composed of human components. While the behaviors within each layer are critical, the increasing dynamism and complexity in system security also includes emergent behaviors at—and across—each layer. Coordinating between several theoretical constructs provides the opportunity to innovate a multiplex approach to system security that could be the foundation for new analytical frameworks, functional requirements, and performance metrics to comprehensively improve next-generation security for high consequence facilities.

1) Physical Protection System Layer: Traditionally the focal point of security efforts, physical protection systems notionally include the collection of physical sensing technologies used to protect a high consequence facility. Examples of such technical components include microwave volumetric sensors, infrared intrusion detection sensors, pan-tilt-zoom visible cameras, and thermal imaging cameras. Current best practices—like DEPO or those proffered by ASIS International [29]—provide guidance on how to select and maintain the capability of each individual component in support of overall security objectives.

Such components are then implemented into a specific arrangement to meet desired security performance outcomes. For example, DEPO emphasizes the need for a collection of PPS components to detect/assess an adversary action and then provide adequate delay to allow a response force to interrupt such malicious actions. To meet these goals, physical protection best practice is to arrange technological components to report signals to a central alarm station (CAS) where disparate pieces of information can be evaluated, related decisions made, and commands executed. An example of the PPS layer is shown in figure 1 (a). Sensing nodes for a demonstrative physical security perimeter intrusion detection system are shown. Note that sensing nodes do not make in-layer connections amongst each other. Though traditionally modeled independently, it is important to note the role of digital (e.g., signal communications) and human (e.g., incoming CAS signal evaluation) components related to performance of the PPS layer.

2) Cyber Architecture Layer: With the recent highlighting of cyber-based attacks on high consequence facilities [30], creating, operating, and maintaining a cyber security architecture has risen in importance. Such cyber security architectures are composed of digital components designed to protect information, networks, and digitally-controlled physical processes from adversarial manipulation. Examples of such components include network communication elements such as internet firewalls, internal network access controls, advanced virus/malware detection software, penetration attempt monitoring algorithms, and encrypted information-sharing protocols. More generally, the cyber architecture layer contains all the digital, logical, and computing elements necessary to maintain a secure cyber-physical system. The selection, arrangement, and deployment of such digital components is scalable and flexible to the specific cyber domain protection needs of the high consequence facility.

These digital components are then arranged in a specific manner to achieve pre-defined cyber security objectives. For example, many of these algorithms, protocols, and information access controls are often connected within a cyber security architecture designed to balance protection of digital assets from external manipulation against regional operational business use. Such architectures are designed and constructed to identify, assess, and mitigate potential disruptions—sometimes by removing the disruption and others by quarantining a portion of the digital system. An example of the cyber architecture layer is shown in figure 1 (b). The logical relationships of computing elements and data flow are represented by a series of nodes that aggregate data towards a central ring of communication elements. Though traditionally evaluated independently, this layer is influenced by others, including the need for electrical power from the infrastructure layer and regular use of digital components by humans in the socio-organizational layer.

3) Infrastructure Layer: A strong uderlying infrastructure is necessary to support high consequence facility security. As the underlying skeleton, infrastructure components provide the necessary operating conditions on which other security components rely. For example, infrastructure components can provide the necessary type of electrical power (e.g., 110 volts vs. 220 volts), temperature control (e.g., for vital computer server rooms), and stable structures for physical support.

Civil engineering best practices are used to select and arrange infrastructure components to meet overall—including security-related—objectives. Though not typically described in such terms, a simple model of these infrastructure components is a sparsely connected, simple network illustrating the disparate relationships within this layer. An example of the infrastructure layer is shown in figure 1 (c), with an emphasis on the power system. Power nodes radiate from a central redundant power grid and backup power node element. In addition to leveraging network theoretic measures to describe infrastructure performance, such a model creates a dedicated layer to represent many of the resources (and needs) underlying security at high consequence facilities.

4) Socio-organizational Layer: Lastly is the need to include the various social and organizational elements necessary to provide security at high consequence facilities. Examples of such elements include organizational structures (e.g., where

the security department is located), procedures/policies (e.g., internal security rules), regulations (e.g., external security rules), patterns of behaviors (e.g., adherence to security rules), and management actions (e.g., a demonstrated commitment to security). One traditional approach to selecting, implementing, and evaluating socio-organizational elements is the concept of "security culture" [31], [32], which provides a potentially useful framing of how such elements can help protect high consequence facilities.

Many of the important elements within this layer can be represented using individuals as the components and various characteristics of connectedness between nodes in a network. For example, an organizational chart reflects how individuals are arranged to achieve security goals. Or, consider how formal and informal relationships between members of the security department thought the organization illustrates patterns of behaviors indicative of how important security is within an organization. An example of the socio-organizational layer is shown in figure 1 (d). Operators, commanders, and in-field security personnel are represented in this example.

Invoking network theoretic characteristic and performance measures provides a useful mechanism for evaluating performance of the socio-organizational layer in meeting security objectives. While such socio-organizational influences are difficult to account for they are far from independent as human interactions are necessary for each of the other layers to be successful.

5) In-Layer Interactions: The performance of each of these layers includes more than just the ability for each of the constituent components to achieve individual functional objectives. The traditional detection, delay, and response security objectives are more accurately described as system-level behaviors. For example, detection is not only the ability of a given sensor to identify and measure motion with its measurement field, but rather results from the interactions between all sensors identifying potentially malicious or undesired motion.

In the proposed multiplex-based approach, each of the previously described layers is represented as graphs in an initial attempt to better incorporate such interactions. Using classic network graphs provides a clear, well established paradigm for describing component-to-component interactions, as well as how these interactions and the individual component performance can impact higher level behaviors.

6) Between-Layers Interactions: Yet, there is still a need to investigate multilayer connections. More specifically, modeling each layer—as described above—provides the opportunity to invoke multiplex logic to better understand higher level, more complex interactions on system security. As introduced in the individual layer descriptions above, a more comprehensive framework for system security must include interactions between layers. For example, the interaction(s) between communication elements (in the cyber architecture layer) and sensing components (in the PPS layer) represent individual component connections between distinct layers. Yet, the connection between all digital elements in the cyber architecture layer and electrical power in the infrastructure layer represents an individual component (power supply) to multiple component (digital elements) connection. Another type of between layer interaction is represented in the regular use of physical sensors (in the PPS layer) by operational and security personnel (in the socio-organizational layer)—representing an interesting case of multiple component to multiple component connection.

IV. Hypothetical High Consequence Facility Security Model Discussion

In order to analyze these concepts, a hypothetical security system for perimeter intrusion detection was modeled. The modeled system began with the foundational elements common to most physical security systems as well as key requirements for the demonstrative analysis, as described by Garcia [6]:

- The perimeter is divided into five regions called sectors
- Each sector contains three different sensing devices and one camera
- A communication loop connects hardware in each sector at a junction box to neighboring sector junction boxes
- Both a primary command control display equipment (CCDE) and secondary CCDE exist within the system
- Both a primary video management system (VMS) and secondary VMS exist within the system
- Power enters from the grid at one location, and a secondary power backup system exists
- The primary CCDE system is staffed by central alarm station (CAS) operators and one CAS commander
- The second CCDE system is staffed by secondary alarm station (SAS) operators and one SAS commander
- The CAS commander can direct the actions of security personnel acting as response force

Once these key nodes were established the relational interactions among the constituent elements (i.e., edges) were determined with the graph-based model shown in Figure 2.

Typical security perimeters are divided into sectors which contain a set of sensing devices for detection. Sensors are used to detect adversary action within the sector, with the resultant data reporting back to the CCDE for analysis by the CAS and SAS operators. Logically, sensors must have three properties to function: a communication path back to the alarm processing node (or backup), a power path back to the power grid node (or backup), and the sensor must be configured correctly and functioning, represented by an associated alarm node. Sensing elements pass alarm data to the CCDE, as well as aggregate power and communication via a junction box associated with the sector. Power connections from junction boxes connect to the power grid and a backup power system. Communication from junction boxes are connected together in a loop, with the primary and secondary CCDE system connecting via a single link into the junction box communication loop.

Cameras are present in each sector, and are used to perform assessment of the source of a sensor alarm. Camera data is used by the CAS and SAS operators to assist in determining if a sensor alarm is a true positive (i.e., adverary action of

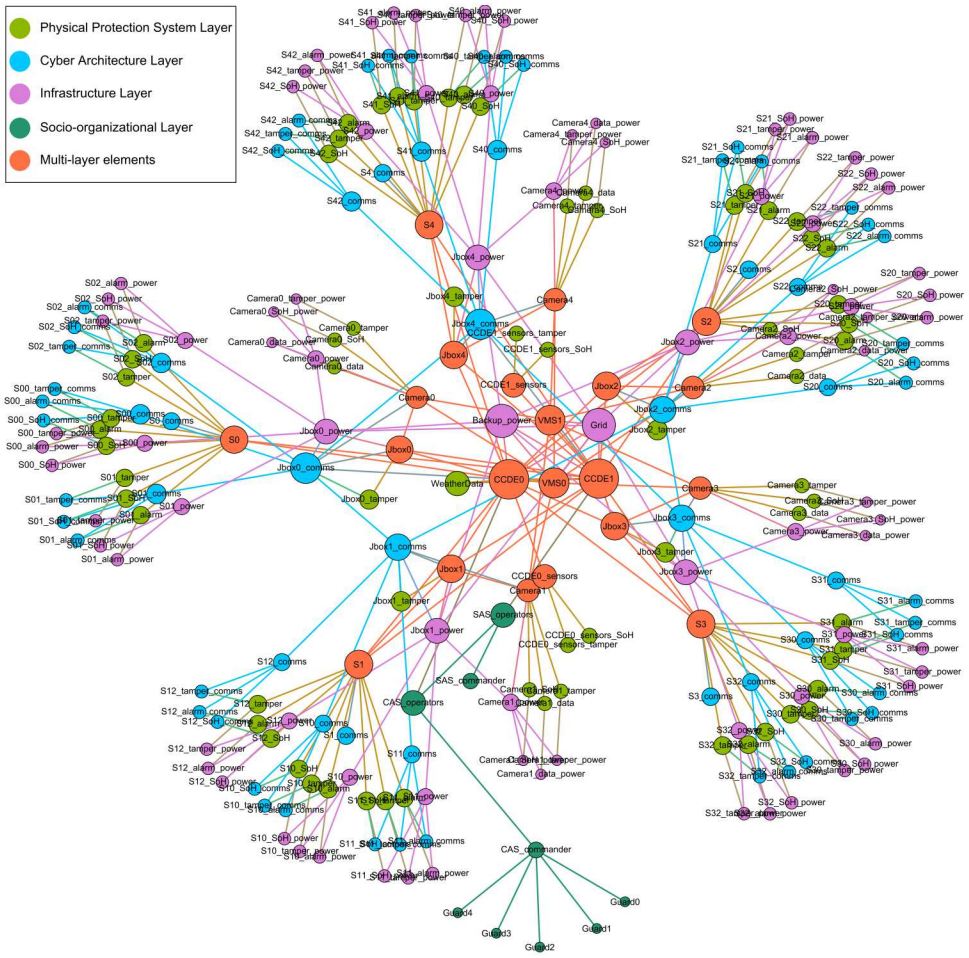


Fig. 2. Example physical security system for perimeter intrusion detection modeled as a graph. Node color is determined by the layer in which the element exists, while node size is determined by the closeness centrality metric. Orange elements cross multiple layers, and are represented as a single color for visual simplification.

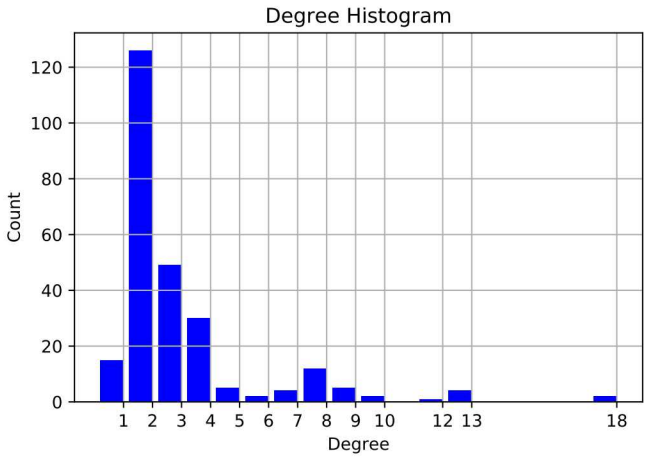


Fig. 3. Degree histogram showing the number of nodes in the physical security network with a given degree.

interest) or a false positive (i.e., a sensor nuisance alarm, such as animals). Camera data must also connect to the primary and secondary VMS. Similar to sensors, cameras must have communication and power paths to the VMS and power grid, respectively. The VMS and CCDE elements make a final communication and data connection between each other.

Additional sensed data exists within the hypothetical system, such as tamper alarm data from various components. These elements must follow the same requirements as sensors and cameras by having communication and power paths back to source nodes as well as an associated alarm node.

A. *Security Analysis of the Graph Model*

Figure 2 indicates that elements in the example physical security system tend to aggregate towards more highly centralized nodes, with the CCDE, VMS, and power grid being critical nodes in this network. Nodes at the perimeter of the network tend to have fewer connections, while nodes in the center behave more as critical hubs of capability and information aggregation. This has implications in both the analysis and design of the system – for example, graph analysis could

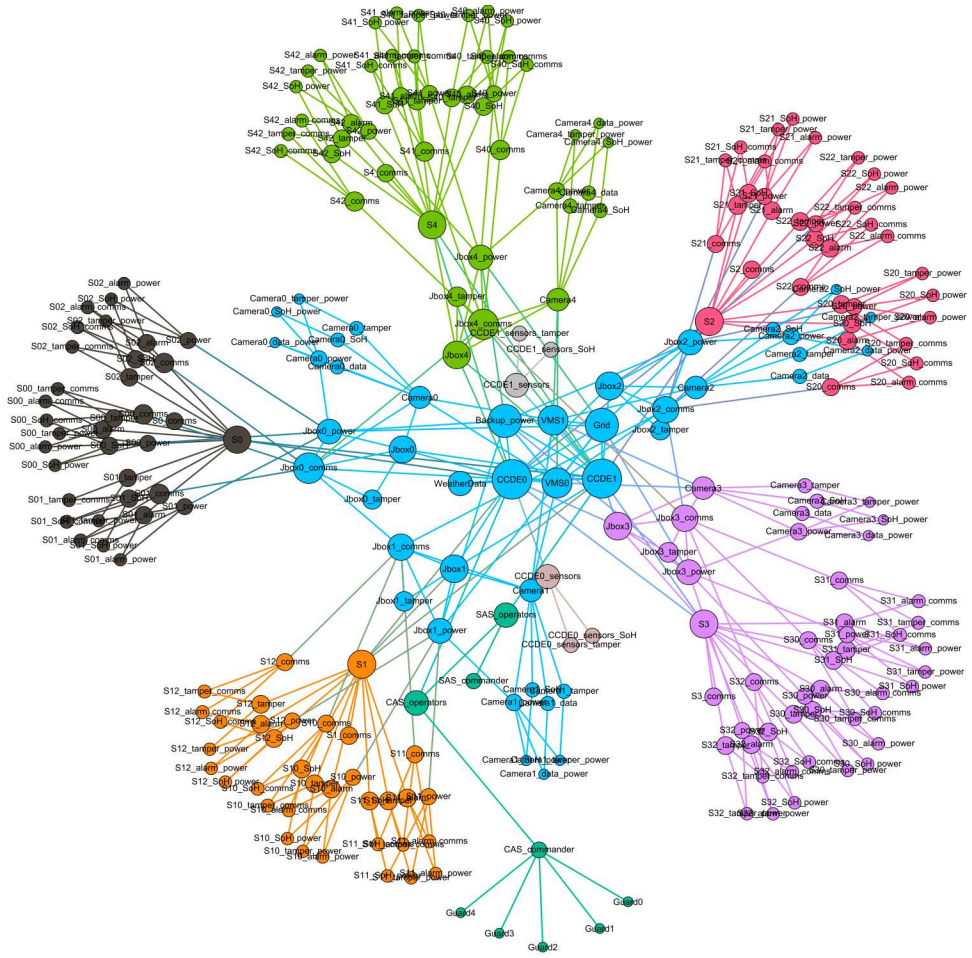


Fig. 4. Example physical security graph showing the nine detected communities. Colors represent nodes in a particular community. Boundaries from community detection isolate sectors, capability and data aggregators, and the socio-organizational elements.

identify nodes or communities whose isolation in the network make the overall security system more susceptible. Alternative system architectures could also be investigated that reduce capability and information aggregation, instead investigating a more decentralized security architecture to improve security performance and resiliency.

Figure 3 shows the degree histogram for the system security network shown in Figure 2. The average degree for this graph is 3.35 with an average path length of 4.51; thus, this example network contains a significant number of nodes with only two connections, primarily from data collection elements associated with sensors and cameras. Conversely, there are a low number of nodes with very high degree (e.g., the primary and secondary CCDE) that are important elements of the security system whose failure could have significant consequences. Knowledge of average degree and path length is also useful for determining more meaningful probabilities of element performance, especially when a system is under degraded operating conditions. Additionally, the impact of path length and number of edges versus traditional (e.g., probability of detection) and advanced (e.g., resiliency) system-level metrics can now be evaluated in order to understand the more complex interactions that occur in a highly interdependent security system.

Figure 4 shows the results of an initial investigation into the characteristics of the multi-layered graph. The Blondel et al. algorithm [33] for community detection was performed. Using this technique for clustering based on the relative density of internal and external edges between nodes, nine communities were detected. The resultant clusters map closely to the sectorized security system introduced for the hypothetical facility and identify additional communities within the network. Identifying the implemented sectors demonstrates parsimony of multiplex-based approaches (and analysis techniques), as well as highlighted additional communities whose properties could be modified to improve overall system security.

For example, if the goal of a physical security system is to maximize its ability to function even under degraded conditions, the large number of low degree nodes and the high closeness centrality for critical elements such as the CCDE system, VMS, and the power grid and power backup may indicate connection types whose modification could improve system-level behaviors. Additionally, the presence of redundant communication loops, CCDE nodes, and power nodes

likely improves the resiliency of the system. The model is also useful for identifying distinct bottlenecks in the system such as the junction box components.

V. Conclusions and Implications

Challenges to current security approaches suggest a need to incorporate interactions observed within system security performance to mitigate increasing real-world complexity and loss of environmental control. Using a multiplex-based approach to leverage key concepts from resilience science, complex system theory, and network theory domains resulted in several new insights. First, system security design and analysis should incorporate adversary mitigation efforts at the PPS, cyber architecture, infrastructure, and socio-organizational layers. Second, incorporating multi-domain interactions provides higher fidelity understanding of observed system security behaviors, as demonstrated by the correlation of the clustering algorithm, identified communities in the multiplex to the sectors in the hypothetical facility. Lastly, network-based models expand the analytic solution space for system security. For example, how measures of centrality between multiplex nodes can identify previously unidentified shortcomings in – as well as overlooked opportunities to improve – systems performance.

This initial analysis of a multiplex-based approach to system security is the first step toward identify conceptual, technical, and analytical needs to improve development and deployment at high consequence facilities. These promising results indicate that a multiplex-based approach is capable of helping system security shift from a "reactive" to "proactive" paradigm. Further research is necessary to identify and explore such dynamism—particularly in terms of incorporating novel insights from the growing resiliency literature. Ultimately, this multiplex-based system security model will help protect high consequence facilities in complex, nonlinear environments, versus innovative adversaries, and against disruptive technologies.

References

[1] W. Q. Bowen, M. Cottee, C. L. Hobbs, L. Lentini, M. Moran, and S. Tzinieris, *Nuclear Security Briefing Book*. King's College London, UK, 2014.

[2] A. D. Williams, "Beyond gates guards and guns: The systems-theoretic framework for security at nuclear facilities (phd defense slides).," tech. rep., Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2018.

[3] A. D. Williams, "The importance of context in advanced systems engineering," *Systems Engineering in the Fourth Industrial Revolution: Big Data, Novel Technologies, and Modern Systems Engineering*, 2020.

[4] "Program on technology innovation: Analysis of hazard models for cyber security, phase i," tech. rep., Electric Power Research Institute, 2015.

[5] N. Firth, "A coordinated drone attack has knocked out half of saudi arabia's oil supply," 2019.

[6] M. L. Garcia, *Design and Evaluation of Physical Protection Systems, Second Edition*. Newton, MA, USA: Butterworth-Heinemann, 2nd ed., 2007.

[7] A. Williams, D. Osborn, K. Jones, E. Kalinina, B. Cohn, M. Thomas, M. Parks, E. Parks, B. Jeantete, and A. Mohagheghi, "System theoretic frameworks for mitigating risk complexity in the nuclear fuel cycle: Final report (sand2017-10243)," *Sandia National Laboratories, Albuquerque, NM*, 2017.

[8] A. D. Williams, "Beyond a series of security nets: applying stamp & stpa to port security," *Journal of Transportation Security*, vol. 8, no. 3-4, pp. 139–157, 2015.

[9] D. e. a. Callow, "Physical security system of the future: Vision and roadmap-official use only," tech. rep., Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2016.

[10] T. e. a. Gunda, "An organization selection tool for security integrated assessments-official use only," tech. rep., Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2018.

[11] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez, "A review of definitions and measures of system resilience," *Reliability Engineering & System Safety*, vol. 145, pp. 47–61, 2016.

[12] B. Biringer, E. Vugrin, and D. Warren, *Critical infrastructure system security and resiliency*. CRC press, 2013.

[13] J.-P. Watson, R. Guttromson, C. Silva-Monroy, R. Jeffers, K. Jones, J. Ellison, C. Rath, J. Gearhart, D. Jones, T. Corbet, *et al.*, "Conceptual framework for developing resilience metrics for the electricity oil and gas sectors in the united states," *Sandia National Laboratories, Albuquerque, NM (United States), Tech. Rep*, 2014.

[14] E. D. Vugrin, D. E. Warren, M. A. Ehlen, and R. C. Camphouse, "A framework for assessing the resilience of infrastructure and economic systems," in *Sustainable and resilient critical infrastructure systems*, pp. 77–116, Springer, 2010.

[15] P. Ferreira, "Mit esd.83 research seminar in engineering systems: Tracing complexity theory," 2001. URL: http://web.mit.edu/esd.83/www/notebook/Complexity%20Theory.ppt.

[16] W. Weaver, "Science and complexity," *American scientist*, vol. 36, no. 4, pp. 536–544, 1948.

[17] L. Von Bertalanffy, "The history and status of general systems theory," *Academy of management journal*, vol. 15, no. 4, pp. 407–426, 1972.

[18] J. Rasmussen, "On the structure of knowledge a morphology of mental models in a man-machine system context riso-m-2192," *Riso national laboratory, DK-4000 Roskilde, Denmark*, 1979.

[19] M. Mitchell, *Complexity: A Guided Tour*. New York, NY, USA: Oxford University Press, Inc., 2009.

[20] J. P. Hecker and M. E. Moses, "Beyond pheromones: evolving error-tolerant, flexible, and scalable ant-inspired robot swarms," *Swarm Intelligence*, vol. 9, no. 1, pp. 43–70, 2015.

[21] T. Flanagan, W. Beyeler, D. Levin, P. Finley, and M. Moses, "Movement and spatial specificity support scaling in ant colonies and immune systems: Application to national biosurveillance," in *Evolution, Development and Complexity*, pp. 355–366, Springer, 2019.

[22] C. Hidalgo, "A tale of two literatures: An antidisciplinary review of social networks and network science." Shared in MIT Course MAS.581-Networks, Information and the Evolution of Complex Systems, 2014.

[23] Y.-Y. Liu, J.-J. Slotine, and A.-L. Barabási, "Control centrality and hierarchical structure in complex networks," *Plos one*, vol. 7, no. 9, p. e44459, 2012.

[24] A. D. Williams and K. A. Jones, "Invoking network & system theory to improve security risk management in international transport of spent nuclear fuel.," tech. rep., Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2017.

[25] M. Kivelä, A. Arenas, M. Barthelemy, J. P. Gleeson, Y. Moreno, and M. A. Porter, "Multilayer networks," *Journal of complex networks*, vol. 2, no. 3, pp. 203–271, 2014.

[26] F. Battiston, V. Nicosia, and V. Latora, "Structural measures for multiplex networks," *Physical Review E*, vol. 89, no. 3, p. 032804, 2014.

[27] S. Gomez, A. Diaz-Guilera, J. Gomez-Gardenes, C. J. Perez-Vicente, Y. Moreno, and A. Arenas, "Diffusion dynamics on multiplex networks," *Physical review letters*, vol. 110, no. 2, p. 028701, 2013.

[28] J. Gómez-Gardenes, I. Reinares, A. Arenas, and L. M. Floría, "Evolution of cooperation in multiplex networks," *Scientific reports*, vol. 2, p. 620, 2012.

[29] *Facilities physical security measures guideline*. ASIS International, 2009.

[30] T. Ball, "Top 5 critical infrastructure cyber attacks," 2017.

[31] I. Khripunov, "A culture of security: Focus for the next nuclear security summit?," 2015.

[32] N. A. of Sciences, *Brazil-U.S. Workshop on Strengthening the Culture of Nuclear Safety and Security: Summary of a Workshop*. The National Academies Press, 2015.

[33] V. D. Blondel, J.-L. Guillaume, R. Lambiotte, and E. Lefebvre, "Fast unfolding of communities in large networks," *Journal of statistical mechanics: theory and experiment*, vol. 2008, no. 10, p. P10008, 2008.