EasyChair Preprint

№ 6810

Resilience-Based Performance Measures for Next-Generation Systems Security Engineering

Adam Williams, Thomas Adams, Jamie Wingo, Gabriel Birch, Susan Caskey, Elizabeth Fleming and Thushara Gunda

October 8, 2021

Resilience-Based Performance Measures for Next-Generation Systems Security Engineering

Adam D. Williams, Thomas Adams, Jamie Wingo, Gabriel C. Birch, Susan A. Caskey, Elizabeth S. Fleming, and Thushara Gunda
Global Security & Integrated Security Solutions Divisions, Sandia National Laboratories, Albuquerque, NM, USA
[adwilli, thoadam, jwingo, gcbirch, sacaske, eflemin, tgunda]@sandia.gov

***Abstract*—**Performance measures commonly used in systems security engineering tend to be static, linear, and have limited utility in addressing challenges to security performance from increasingly complex risk environments, adversary innovation, and disruptive technologies. Leveraging key concepts from resilience science offers an opportunity to advance next-generation systems security engineering to better describe the complexities, dynamism, and non-linearity observed in security performance—particularly in response to these challenges. This article introduces a multilayer network model and modified Continuous Time Markov Chain model that explicitly captures interdependencies in systems security engineering. The results and insights from a multilayer network model of security for a hypothetical nuclear power plant introduce how network-based metrics can incorporate resilience concepts into performance metrics for next generation systems security engineering.

***Keywords*—** *Systems security engineering High consequence facility security, Resilience, Multilayer networks*

I. Introduction

Advances in systems security engineering focus on incorporating a socio-cyber-physical paradigm that describes security performance in terms of interaction between people, procedures, technologies, and environments [1]. Where some related approaches define security performance as effectiveness of individual sensors or sectors, other approaches argue that security performance emerges from interactions between sensors and sectors. In other words, security performance is *not only* a microwave sensor alarming *or* a steel reinforced wooden door *or* an armed protective force deploying to a conflict situation—effective security results from *both* their individual operation and the interactions *between* the operations of these sensors and sectors. From this perspective, next-generation systems security engineering should produce performance measures more amenable to the dynamism, non-linearity, and complexity observed in current threat environments—particularly for high consequence facilities.

High consequence facilities (HCF), according to the U.S Department of Homeland Security (DHS), are "those whose incapacitation would have a devastating impact on national security, economic prosperity, and/or public health" [2]. Given the potential scale for significant disturbance to chemical, defense, energy, and medical facilities, next-generation systems security engineering will need to mitigate additional sources of uncertainty to protecting critical infrastructure, including (but not limited to):

- Increased digitization in HCF controls [3];
- HCF deployment to non-traditional, more remote locations [4];
- The impacts of organizational/individual inertia on [5];
- Cyber attacks on critical pieces of infrastructure [6] [7];
- Increased evidence of "violent extremists have, in fact, obtained insider positions" in HCF [8];
- The use of advanced unmanned aerial systems to attack HCF [9]; and,
- Anticipated threats from deep-fakes and malicious artificial intelligence [10].

Collectively, these additional sources of uncertainty in security engineering represent new challenges to be address based on increasingly complex risk environments, adversary innovation, and disruptive technologies. These challenges also call into question the efficacy of traditional security performance metrics to adequately describe security system performance. Here, borrowing from advances in resilience science, complexity theory, and network science provides useful insights for better addressing these challenges. Multilayer networks—described capturing interactions between related networks that provides a much more comprehensive view of complex systems [11]—seem able to provide a mathematically tractable approach enhancing more traditional security metrics with resilience concepts to address and mitigate match these challenges to desired security system behaviors

II. Security System Performance Metrics

A. Traditional Security Approaches

One popular HCF security framework—the Design Evaluation Process Outline (DEPO)—was developed by Sandia National Laboratories (Sandia) in the late 1970s and early 1980s. Though developed in response to a 1973 Congressional mandate to improve the security of nuclear materials [12], DEPO is commonly applied to meet various HCF security needs. DEPO heavily leverages the analytical successes in nuclear safety, including borrowing the use of sets of conditional

978-1-7281-1576-4/19/$31.00 ©2019 IEEE

probabilities to mathematically describe how well a collection of security components detect, delay, and respond to specific adversaries along specific paths [13]. The DEPO framework serves as the basis for current state-of-the-art HCF path analysis techniques. Such techniques evaluate and prioritize security system performance in terms of detection, delay, and response performance metrics against a specific adversary skillset along a specific pathway toward an HCF target.

The DEPO framework and associated path analysis techniques leverage this detect, delay, respond paradigm to fully describe HCF security system performance. Component-level performance metrics typically only include the probability of detection (P_D), delay time (t_D), and response force time (RFT). More specifically, the DEPO methodology uses P_D and t_D to describe the ability of a security system to "detect" and "delay" adversary actions along a particular path—combining them into the compound probability of interruption (P_I). Similarly, the DEPO methodology describes the ability for security systems to "respond" and muster sufficient protective forces to mitigate the adversary actions as the compound probability of neutralization (P_N). The resulting primary performance measure is called "system effectiveness (P_E)," and represents a simplified combination of PI and PN in a modified generic risk equation. Yet, for each of these traditional DEPO-related performance measures, these probabilities are calculated assuming that the separate detection, delay, and response actions are independent.

Despite its widespread use and success over the last few decades, DEPO—and its associated path analysis techniques—struggle to account for the previously discussed set of challenges to securing HCF. Described succinctly in a recent "Physical Security System of the Future" technical report from Sandia National Laboratories,

> The design of physical security systems relies heavily on analysis and modeling/simulation of the potential design…Analysis methodologies used today are based on 30-year old Cold War technologies and threats. The methodologies used are *not flexible or adaptable, and they limit options* to improve system effectiveness… Current systems fail to incorporate physics based models of sensors and imagers, which prevents systematic analysis of different physical security designs, tradeoffs, data fusion analyses, and human factors studies. [14] (emphasis added)

Thus, there is a need to expand beyond a classic DEPO-based approach to address the pace of technological, organizational, societal, and political challenges and toward approaches that better characterize HCF security in more dynamic, interdependent terms.

B. Key Resilience Concepts

Resilience science offers a paradigm, set of concepts, and range of performance measures seemingly capable of addressing these gaps in more traditional DEPO-based approaches. In generic terms, resilience of complex systems refers to the capacity and ability to return to a stable state after a disruption [15]. In this manner, resilience science describes emergent performance in terms of meeting overall system objectives under ideal, nominal, and sub-nominal conditions. This emphasis on recovery affords a better opportunity to address additional sources of uncertainty that change over time. Conceptually, resilience can be described as a restorative capacity that is a function of the absorptive and the adaptive capacity of a complex system. The absorptive capacity describes the degree to which a system can withstand perturbations with minimal effort, while the adaptive capacity captures the degree to which a system can dynamical self-(re)organize to return to acceptable operations [16].

Given the anecdotes representing challenges to HCF security presented in the opening section, security system performance is a dynamic parameter that seemingly captures elements of prevention, protection, defense, and recovery. Thus, incorporating these resilience concepts helps extend the concept of "security" from simply focusing on preventing and defending against malicious to more broadly supporting and maintaining HCF base operations. For example, this resilience-based perspective argues that adequate HCF security results from both high system effectiveness and ensuring HCF operations—suggesting that metrics describing disruptive impact on system performance are applicable to describing HCF security performance. Similarly, metrics depicting the resource and time needs to complete recovery back to previous (or new acceptable) system operations also seem applicable to HCF security [16]. Fig. 1 offers conceptual visualizations for such resilience-based metrics for HCF security.

Invoking a resilience paradigm provides additional concepts by which to capture—and mathematically describe—the dynamism, complexity, and non-linearity observed in today's HCF security performance. Recharacterizing HCF security performance as dynamic metrics ranging from prevention to recovery helps capture the interactions observed between HCF operations, operational contexts, HCF security system designs, and previously described challenges. In addition, incorporating

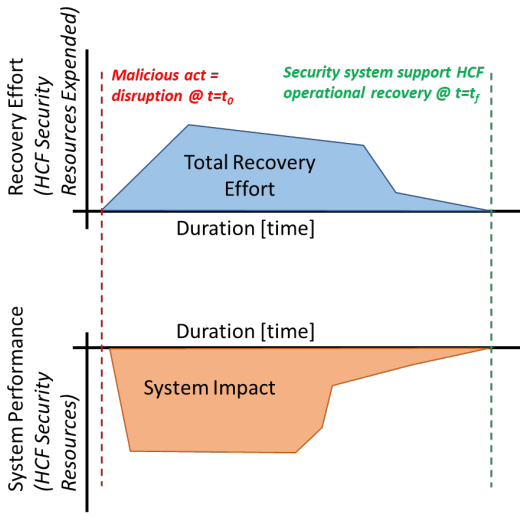

Fig. 1. Conceptual representation of resilience performance metrics and their logical relationships to HCF security performance (recreated from [16]).

resilience concepts also helps steer away from seeking singular, "independent" root causes and toward more dynamic, interdependent explanations of observed HCF security design and analysis outcomes.

C. Multilayer Networks

In addition, network theory provides helpful concepts, frameworks, and approaches to combine key elements of resilience science with HCF security. In the broadest sense, network theory identifies, characterizes, prioritizes, analyzes, and optimizes complex system behaviors by defining and measuring interactions between components. This is conceptually similar to how DEPO-based approaches to HCF security articulate relationships between detection, delay, and response components. Network models are also helpful in describing how these interactions and relationships characterize non-linear behaviors observed in complex systems. Here, network models expand on traditional DEPO-based approaches by capturing interactions between detection, delay, and response components, as well as offering more mathematical descriptions of priority, importance, and communication among nodes in HCF security system.

Recent advances in network theory have described, measured, and evaluated the emerging behaviors observed in networks consisting of multiple, interacting layers [11]—hereafter referred to as "multilayer networks (MLN)." For HCF security, this seems consistent with the (often ignored) interactions between physical security designs, cyber security architectures, and personnel security programs. One benefit of MLN models for HCF security, then, would be the ability to visualize how components within and across layers can interact and result in unexpected—yet, potentially designable—performance measures. Such a MLN modeling approach also seems well positioned to incorporate resilience-related concepts and performance metric elements. A MLN-based approach also helps take advantage of a larger portion of generated data during HCF security operations and introduces capabilities to capture potential performance measures describing relative importance between components in sector of a security system, the prioritization of sectors within a security system, or aspects of absorptive, adaptive, and restorative capacity.

Coordinating these concepts toward developing MLN models for HCF security offers opportunities to capture the multidomain interactions observed in real security scenarios [17][18]. Consider, for example, MLN multilayer communicability, a metric defined as "a centrality measure which quantifies the number of paths taking both Intralinks [within a layer] and interlinks that join a given node of a given layer to the other nodes of the multilayer structure" [11]. This metric seems to describe the potential for manipulation of digital components to cascade across other security system domains (represented as layers) and cause unexpected/undesired behaviors in physical security components. Multilayer communicability also speaks to restorative capacity for HCF security systems, as intentional disruptions of components with higher values of this performance metric will have more negative impacts on system operations and take more time and resources to adequately recover.

III. Multilayer Network Models: Security Examples

A. Hypothetical Nuclear Power Plant Description

The Lone Pine Nuclear Power Plant (LPNPP) is a two-loop pressurized light water reactor (PWR) with a reactor power level of 1150 megawatts electric at full power that operates 24 hours, 7 days a week. The system consists of a reactor, a closed primary coolant loop connected to the reactor vessel, and a closed separate power conversion system (secondary coolant) for the generation of steam to power the turbine(s). Significant buildings and operations at the facility include the Reactor Containment Building, Auxiliary Building, Engineered Safety Features (ESF) Building, Control Building, Condensate Storage Tank and Piping, and the Fuel Building—as shown in site layout provided in Fig. 2. The associated security system 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) elements commensurate with international best practices for protecting nuclear plants [19].

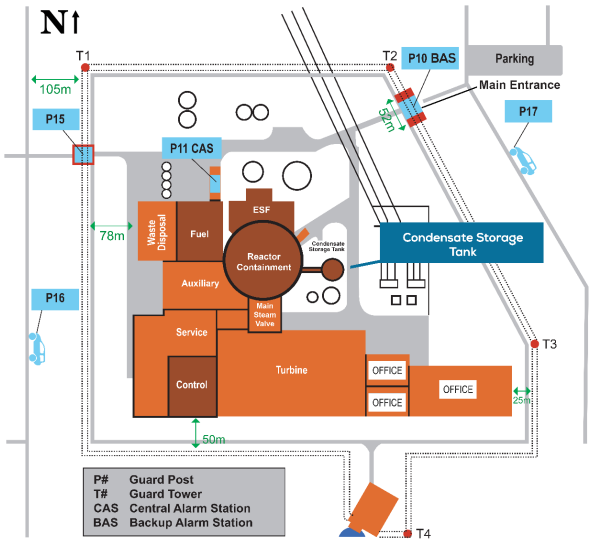

Fig. 2. Two-dimensional overview & site layout of the hypothetical Lone Pine Nuclear Power Plant [19].

B. Network Representation & Simulation

Security subject matter expert knowledge was used to identify where specific security components such as sensors, network components, power systems, and aggregating junction boxes would exist in the LPNPP model. To capture the features of the different edge types present within the system, this multilayer network is represented as multi-edge connections between nodes, with each edge representing relationships between data/communications, delivering power or human interactions with a component. The layers in this MLN model each contain edges where each component in the system is represented on every layer as replica nodes. The edges between replica nodes are used to convey the bi-directional influence between component different layers. In general, edges are built using logic determined by common security system configurations. For example, communication network

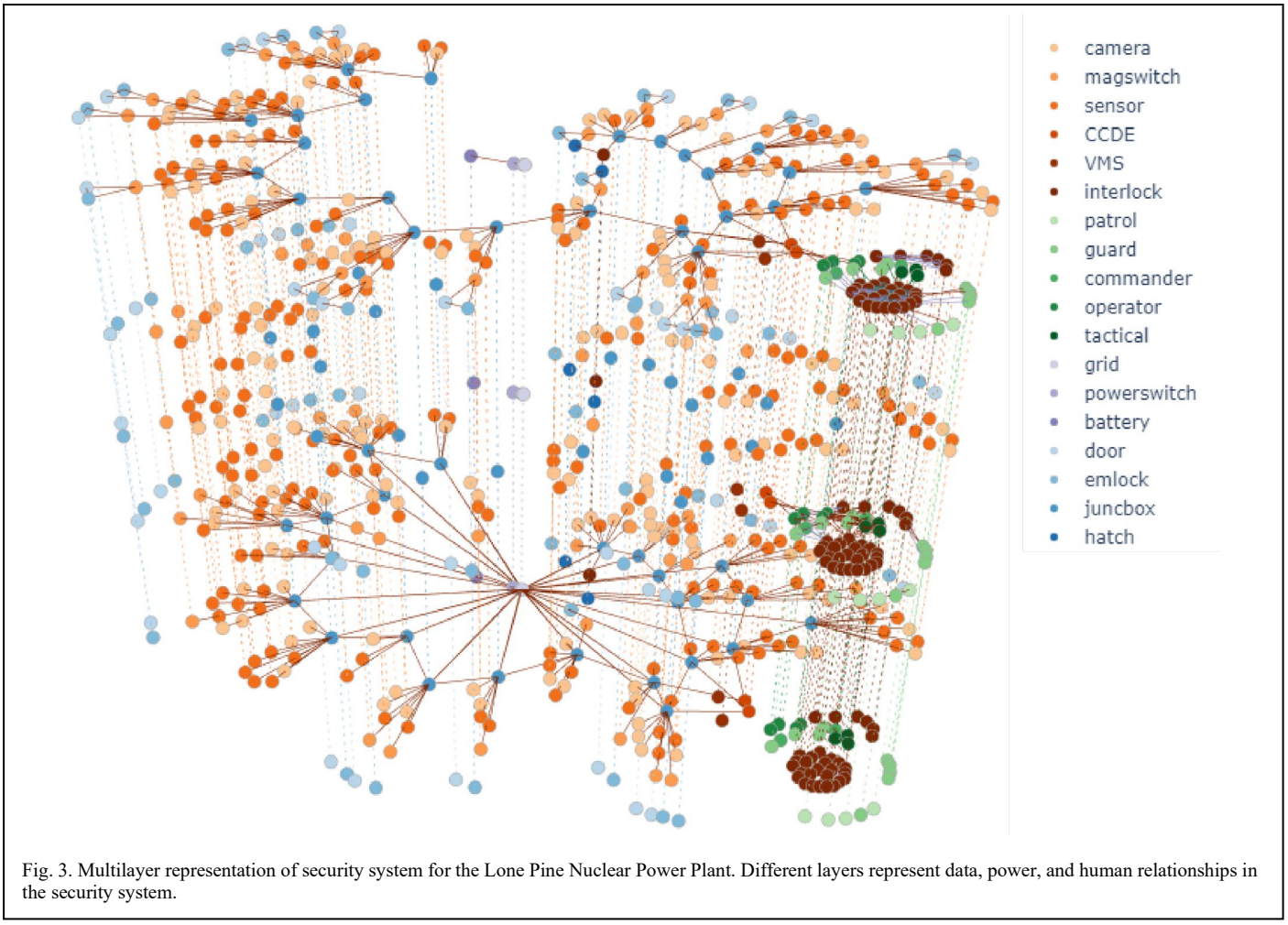

Fig. 3. Multilayer representation of security system for the Lone Pine Nuclear Power Plant. Different layers represent data, power, and human relationships in the security system.

configuration typically has sensors and cameras reporting to network switches in junction boxes, which then travel across a backbone network to the central alarm station (CAS) and secondary alarm station (SAS). The MLN representation in Fig. 3 captures this by having nodes with data edges between sensors and junction boxes, data edges between adjacent junction boxes, and some portion of junction boxes ultimately having data edges to the CAS and SAS. Each perimeter intrusion detection sector contains a minimum set of data generator nodes (e.g., cameras and sensors), and power connections (e.g., power edges from supply to device). Because aggregating junction boxes are shared by two sectors, junction boxes are therefore physically present in every other perimeter intrusion detection sector.

A multi-agent simulation incorporating the MLN security system model was created to understand the impact of disparate event—ranging from intrusions to infrastructure failure. The simulation is designed to operate with different components on different timescales, capturing unspecified behavior in activities that proceed through multiple domains and components. This necessitated an object-oriented, agent-based continuous time, discrete event-based model of the system. More concretely, the simulation is a modified Continuous Time Markov Chain model in which every action represents a potential discrete event. Examples of these events include messages passing through a junction box, a central alarm station (CAS) operator assessing an alarm, a sensor surveying its surroundings to affect a change in state, or even the degradation of a component. Early evaluation suggests this simulation approach allows holistic modelling of security systems and spatio-temporally defined intruders, enabling analysis of security system performance via Monte Carlo experimentation.

C. Analysis & Results

A series of Monte Carlo simulations was conducted determine the ability of the security system to communicate information back to the CAS and secondary alarm station (SAS) as the overall structure of security system slowly degrades—speaking to absorptive capacity in resilience terms. Using the Lone Pine Nuclear Power Plant MLN model in the absence of any intrusions, random MLN edges were destroyed between two powered devices every 1000 timesteps. This experiment continued until the entire security system fractured and the resulting number of reported nominal signals received by the CAS and SAS dropped near zero. All sensors were set to produce signals at the same rate, enabling this simulation to be interpreted as the proportion of correctly reporting sensors to the CAS and SAS as a function of broken edges (Fig .4).

Removal of random edges within the MLN followed the logic hypothesized in security system operations. For example, removal of a power connection to a junction box would result in

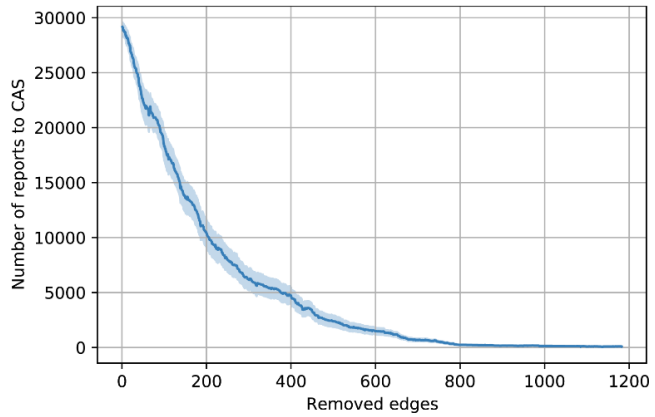

Fig. 4. Number of reports sent to CAS as a function of removed edges. The solid line shows the average number of reports over 64 Monte Carlo simulations, while the shaded region shows the 90th percentile value.

the cascading removal of data edges between sensors connected to the same junction box, as sensors cannot send data without power. A total of 64 repeated Monte Carlo simulations were conducted. Results from these separate simulations were averaged together in order to more effectively understand the impact of removing edges. These results indicate that random edge removal for this particular security system topology generates a non-linear reduction in the number of average messages received at the CAS. This non-linear degradation of system performance speaks to the ability of this HCF security system to adequately absorb a disruption and maintain adequate levels of security operations. As such, this MLN model provides a quantitative measure—and design parameter—by which to incorporate resilience concepts into security performance. Future experiments will look to compare these results of random node removal with more targeted node removal based on such MLN characteristics as multilayer communicability to better mimic potential malicious adversary actions.

IV. Conclusions & Implications

Current results support the modeling of HCF security system performance in terms of multilayer network performance measures. MLN model-based approaches also provide a suite of mathematically tractable metrics to better describe more complex behaviors observed in HCF security. Invoking resiliency concepts and MLN topologies forms the foundation for systems security engineering approaches better able to mitigate the range of challenges facing HCF. Extending recent advances in resilience science and network theory, MLN models provides a viable path for both HCF security and systems security engineering to better address the role(s) of human actors, multidomain interactions, non-linear operational environments, and anticipatory performance measures necessary to mitigate real-world complexities, innovative adversaries, and disruptive technologies.

Acknowledgements

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. SAND2021-12204 C.

References

[1] R. Dove and K. D. Willett, 'Contextually Aware Agile-Security in the Future of Systems Engineering,' IEEE/NDIA/INCOSE Systems Security Symposium (SSS), 2020.

[2] Cyber Infrastructure Security Agency (CISA), 'U.S. Department of Homeland Security: Critical Infrastructure Sectors,' 2020, https://www.cisa.gov/critical-infrastructure-sectors

[3] S. Clayton, 'The modern movement: digital I&C,' The Nuclear Engineering International Magazine', 2018, https://www.neimagazine.com/features/featurethe-modern-movement-digital-ic-6231488/

[4] Nuclear Engineering International, 'Russian floating nuclear plant supplies 10GWh of electricity to Chukotka,' Nuclear Engineering International Magazine, 2020, https://www.neimagazine

[5] A. D. Williams, 'The Improtance of Context in Advanced Systems Engineering,' in Systems Engineering in the Fourth Industrial Revolution, Wiley & Sons, 2019, pp. 45-75.

[6] A. Campbell and V. Singh, 'Lessons from the cyberattack on India's largest nuclear power plant,' Bull. Atom Sci, 2020, https://thebulletin.org/2019/11/lessons-from-the-cyberattack-on-indias-largestnuclear-power-plant/

[7] D. Sanger and N. Perlroth, 'Pipeline Attack Yields Urgent Lessons about U.S. Cybersecurity,' NY Times, 2021, https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html

[8] Homeland Security Newswire, 'DHS warns utilities at risk from insider threats,' News Wire Publications, 2011, < http://www.homelandsecuritynewswire.com/dhs-warns-utilities-riskinsider-threats>

[9] B. Hubbard, P. Karasz, and S. Reed, 'Two Major Saudi Oil Installations Hit by Drone Strike, and US Blames Iran,' NY Times, 2019, https://www.nytimes.com/2019/09/14/

[10] University College London, '"Deepfakes" ranked as most serious AI crime threat', ScienceDaily, 2020, https://www.sciencedaily.com/releases/2020/08/200804085908.htm

[11] G. Bianconi, Multilayer Networks: Structure and Function, Oxford University Press, 2018.

[12] W. J. Desmond, N. R. Zack and J. W. Tape, 'The First Fifty years: A review of the department of energy domestic safeguards and security program', J of Nuclear Matls Mgmt, 1998, 26.

[13] M. L. Garcia, Design and Evaluation of Physical Protection Systems, 2nd ed., Elsevier, 2007.

[14] D. Callow, et. al, 'Physical security system of the future: Vision and Roadmap-Official Use Only', Sandia National Laboratories, SAND2016-12214, 2016.

[15] S. Hosseini, K. Barker and J. Ramirez-Marquez, 'A review of definitions and measures of system resilience," Rel. Eng. & Sys. Safety, 2016, 145, pp. 47-61.

[16] 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 Sust. & Res. Crit. Infra. Sys., Springer, 2010, pp. 77-116.

[17] A.D. Williams, et. al, 'A Complex Systems Approach to Develop a Multilayer Network Model for High Consequence Facility Security', Proc. Int. Conf on Complex Sys, 2020.

[18] A.D. Williams and G.C. Birch, 'A Multiplex Complex Systems Model for Engineering Security Systems', Proc IEEE Sys Sec Symp, 2020.

[19] D. Osborn, et. al, 'Modeling for Existing Nuclear Power Plant Security Regime,' Sandia National Laboratories, SAND2019-12014, 2019.