Governance and Resilience: A Holistic Approach to Systems Security in Complex and Chaotic Environments

Sue Caskey, PhD
Sandia National Laboratories
sacaske@sandia.gov
(505) 284-5095

Adam Williams, PhD
Sandia National Laboratories
adwilli@sandia.gov
(505) 264-5246

Abstract

A systems governance approach emphasizes a holistic perspective that identifies and navigates the interdependencies and conflicts between security and operational needs. Governance is defined as a collection of metasystems that provide the necessary constraints and processes to support, steer, adapt, transform, and sustain a system (Keating et al., 2022). Utilizing the Cynefin framework, which distinguishes between simple, complicated, complex, and chaotic environments (Snowden and Boone, 2007), the article highlights the challenges faced by nuclear power plants in predatory contexts and the importance of integrating security objectives into governance frameworks.

By incorporating security as a fundamental aspect of governance, the article underscores its significance for persistence, adaptation, and transformation in the face of uncertainty. Additionally, it introduces key heuristics of systems security, such as the importance of context, knowledge-based decision-making, and organization-specific sociological factors (Williams and Caskey, 2024). Ultimately, this work provides valuable insights into enhancing resilient operations in complex environments by reinforcing the connection between effective governance and security in systems engineering.

Introduction

Governance plays a pivotal role in ensuring the resilience of complex systems, this includes the system's ability to be secure, particularly in environments characterized by uncertainty, interdependence, and high consequences. Much like Cook's (Cook, 2002), concept of safety as being a characteristic of the system rather than characteristic of their components, security is an emergent property of the system. Nuclear power plants exemplify such complex systems, where security and operational performance—and the interaction between them—are paramount. The anticipated expansion of such facilities (via the "new nuclear renaissance" related to advanced and small modular reactors) suggests a higher likelihood of operating within "predatory environments," consisting of multifaceted challenges like physical threats, cyber vulnerabilities, and sociopolitical pressures. Here, governance frameworks can help such systems adapt to and thrive amidst the complexity and chaos of these challenges.

Governance is understood here as a set of constraints, processes, and feedback mechanisms designed to support, steer, adapt, and sustain the system it oversees (Keating et al., 2022; Keating and Katina, 2023). For nuclear power plants, this perspective aligns with recent research out of Sandia National Laboratories that explored new approaches for capturing the complexity, dynamism, and interdependencies of current—and anticipated—security performance needs for complex systems (Williams, et. al 2023). By also incorporating the Cynefin framework's distinction between simple, complicated, complex, and chaotic domains (Snowden and Boone, 2007), a nuanced governance approach to managing the uncertainty and variability inherent in securing complex systems—including nuclear power plant --emerges.

In this context, resilience is a critical dimension of governance, encompassing persistence, adaptability, and transformation (Caskey, 2024), as well as relating to complex system security. These elements enable systems to maintain functionality under stress, adapt to changing conditions, and evolve to address future challenges. This article leverages theoretical insights from governance frameworks, systems theory, and security heuristics to propose a resilience-based approach for security that is illustrated on nuclear power plants. The approach aligns with emerging paradigms in INCOSE's systems security engineering working group which emphasize trustworthiness, loss-driven strategies, and capabilities-based designs. By advocating for security as an integral part of governance, the paper offers actionable insights for system architects, designers, decision-makers, and operators aiming to enhance system resilience in complex and chaotic environments.

Resilience and Security in System Governance

Traditionally a system's governance was specifically defined to support resilience of the system independent of system security. If, however, security is considered an inherent or emergent property of a system, then we are proposing that a resilient governance directly supports system security, particularly in complex environments. Complex systems engineering defines resilience as the system's capacity to persist, adapt, and transform in response to disruptions; traditional systems engineering reflects that security includes providing protective measures necessary to defend the system from threats (Williams, 2020). NIST offers a broader, and more rigorous, treatment of the security and resilience concepts by arguing that each are involved in protecting system capability and functionality (Ross et al., 2022). As such, the range of measures necessary to safeguard against dynamic threats form the foundation for a governance framework capable of addressing the multifaceted challenges inherent in complex system operations.

In the context of governance, resilience is achieved through the integration of persistence, adaptability, and transformation. Persistence involves the system's ability to maintain critical functions under stress, supported by attributes such as redundancy, resource sufficiency, and robust communication channels. Adaptability reflects the system's capacity to adjust to changing conditions, balancing flexibility with stability to ensure continuity of operations. Transformation emphasizes proactive innovation, enabling the system to evolve and address future challenges through learning, transparency, and forward-thinking strategies.

Conversely, traditional approaches to security often focus on such protective measures as physical barriers, cyber defenses, or personnel protocols in isolation. However, an integrated paradigm recognizes security as an emergent property of the entire system (e.g., NIST SP 800-160, Vol. 1, Rev. 1). By leveraging insights from complex system models (like multilayer network models) and governance frameworks, advanced security approaches can identify and address interdependencies across physical, digital, and human domains. Key principles such as situational awareness, graceful extensibility, and trustworthiness underpin such approaches, ensuring that security measures align with the system's broader objectives.

One of the key insights from systems theory is the importance of feedback mechanisms in enhancing both resilience and security (Castelle et al., 2015). Effective governance incorporates feedback loops that enable real-time monitoring, assessment, and adjustment of system operations. These concepts should also be aligned to the security of the system and not only limited to operational performance. For example, environmental scanning processes can detect emerging threats, while communication channels ensure that this information is rapidly disseminated and acted upon. These feedback mechanisms are essential for maintaining situational awareness and enabling timely responses to disruptions.

The Cynefin framework further informs the governance of resilience and security by emphasizing context-specific strategies of systems to changes and uncertainty (Snowden, 2017). In simple and complicated Cynefin domains, standardized procedures and expert-driven analysis can address predictable challenges. In complex and chaotic Cynefin domains, responses must prioritize adaptive responses and rapid interventions. This contextual adaptability ensures that governance mechanisms remain effective across a range of scenarios, from routine operations to crisis situations.

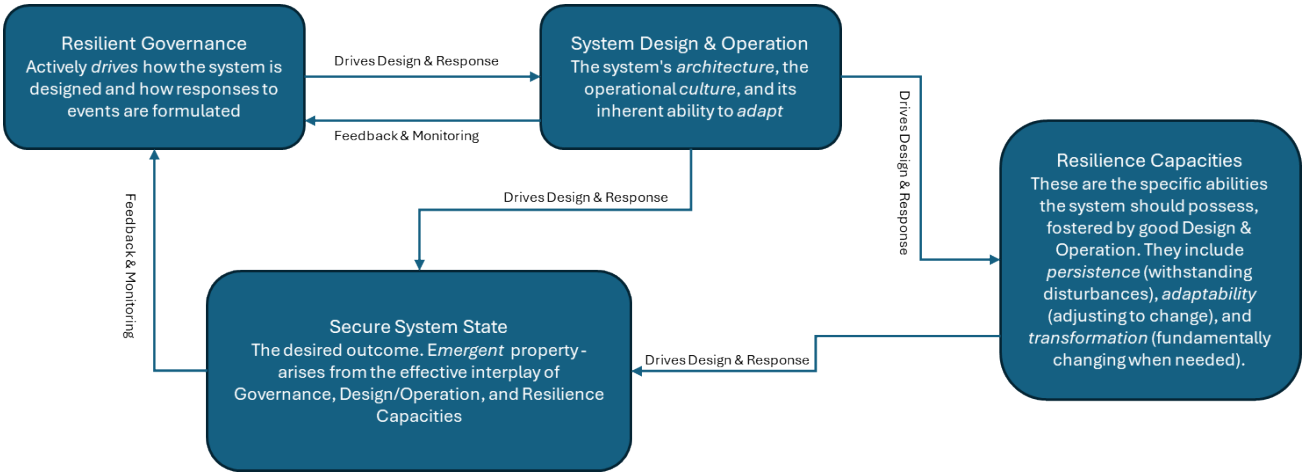

Figure 1 Mental Model Reflecting Relationships between Resilience, Systems Security, and Governance

By integrating resilience and security into a cohesive governance framework (Figure 1), complex systems can better navigate the uncertainties of their operational environments. This approach not only enhances system performance but also mitigates security risks, ensuring the secure and sustainable operation of these systems.

Complex Systems Governance – a New Perspective

The Complex Systems Governance (CSG) framework provides a structured approach to managing systems characterized by interdependencies, variability, and multidimensional challenges. Within this framework, governance is not merely a hierarchical mechanism but an adaptive instrument that facilitates persistence, adaptability, and transformation. These three dimensions form the cornerstone of governance resilience, enabling systems to withstand disruptions, adjust to environmental changes, and proactively evolve to meet emerging demands.

The CSG framework (Figure 2) emphasizes the role of metasystem functions, which provide control, communication, coordination, and integration of a complex system. These metasystem functions ensure that governance not only reacts to immediate challenges but also anticipates and prepares for future perturbations. Drawing on systems theory concepts such as circular causality, requisite variety, and feedback loops, the CSG framework aligns governance mechanisms with the system's operational and environmental complexities. This holistic approach underscores the need for governance to integrate insights from the system’s internal dynamics and external environments.

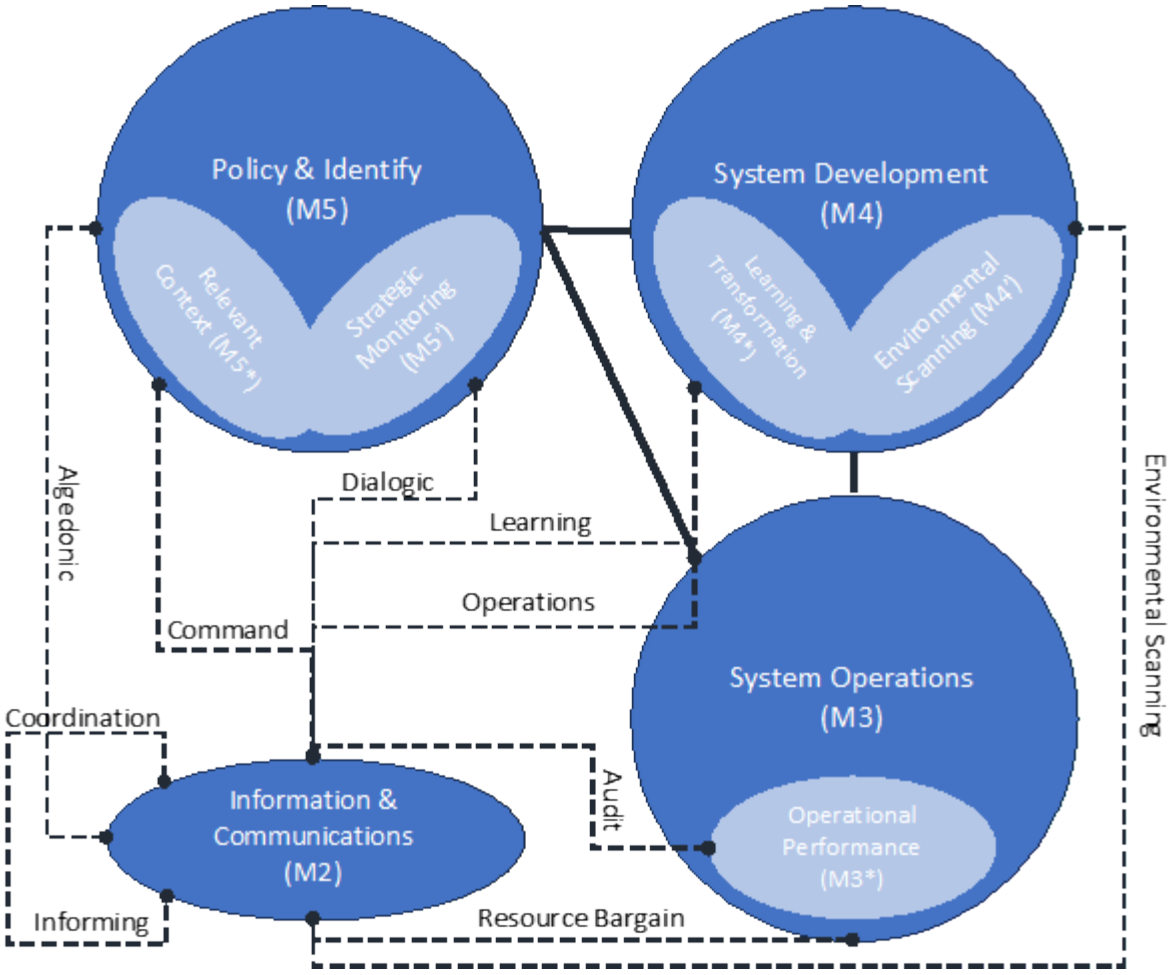

Figure 2 CSG Framework (Keating et al., 2022; Keating and Bradley, 2015; Keating and Katina, 2023)

The Cynefin framework further complements this perspective by categorizing these environments into simple, complicated, complex, and chaotic domains. Effective governance navigates these domains by employing context-appropriate strategies, which can include:

- standardized procedures for simple domains
- expert-driven analysis for complicated domains
- adaptive responses for complex domains
- rapid intervention for chaotic domains

This contextual adaptability is crucial for ensuring resilience in system operations.

Security is also pivotal in the context of resilient operations. Traditional approaches often treat security as a discrete—and somewhat independent—element of system or facility performance. Recent efforts out of Sandia National Laboratories, however, suggest the potential benefit of a governance perspective that integrates security as an emergent and inherent property of a system (Williams & Caskey, 2024). Revisiting Cook's concept of safety being a characteristic of the system rather than characteristic of their components, we postulate that security is an emergent

property of the system—and the more complex the system the more dynamic and uncertain the security of the system. Building off empirically derived security heuristics (Williams & Caskey, 2024), resilient system operations should inherently support security concerns; specifically, those based on principles such as situational awareness, redundancy, and graceful extensibility. These principles align with the governance resilience emphasis on a holistic perspective and ensures that governance mechanisms support both immediate operational needs and long-term system viability.

Table 1 Cynefin Domains and Security-Governance-Resilience Mapping

Domain	Security Need	Common Pitfall	Governance Contribution
Simple	Reliability and vigilance against complacency	Overstandardization; ignoring signs of change	Reinforce routines, monitor for drift, ensure redundancy, support persistency of the system
Complicated	Expert-driven accuracy and layered defense	Technocratic silos; slow to adapt	Coordinate subsystems, integrate expert feedback, maintain procedural integrity; supports persistency and allows for some adaptability in security
Complex	Emergent threat detection and systemic sensing	Over-control; ignoring emergence; premature certainty	Enable distributed sensing, support adaptive response, foster multi-loop learning; in addition to persistency, governance ensures security adaptability and transformation as needed to maintain a secure state
Chaotic	Immediate containment, fast decision-making	Freezing; overanalyzing; unclear decision paths	Preconfigure authority and response; ensure flexible escalation
Disorder	Orientation and domain identification	Forcing a known frame; ignoring divergent views	Foster plural perspectives, meta-sensemaking, structure for coherence

Synthesizing insights from systems theory, the CSG framework, and the Cynefin model introduces a foundation for a governance-based approach to security. For example, security for systems in the “simple” domain will need to focus on reliability of current solutions and vigilance against complacency within those solutions. Table 1., above, summarizes a similar treatment for the other Cynefin framework domain. Yet, an over reliance on standardization and susceptibility to change blindness are common shortcomings experienced in these security solutions. In response, incorporating systems governance provides monitoring for drifts away for desired behaviors and support for persistency that help mitigate this pitfall, resulting in overall

enhanced security solutions. This foundation provides the basis for exploring practical strategies that enhance system security and adaptability, paving the way for innovative governance approaches for complex systems.

Complex System Governance Use Case: Advanced Nuclear Power Plants

The anticipated future of advanced nuclear power plants presents several challenges that could significantly impact resilience in traditional operations commensurate with the long history of nuclear generated electricity. For example, the wide introduction of so-called passive safety systems (or safety mechanisms that do not require external energy for initiation) may not fully address the dynamic and evolving threats hypothesized for (near) future nuclear operations. Similarly, as advanced nuclear power plants incorporate increased digitization, automation, and remote operations, the operational (and security) landscape becomes more complex. While such advancements can enhance operational efficiency, they can also create new weaknesses in operations that must be identified and mitigated to ensure resilience. These facilities operate in environments where the potential consequences are exceptionally high, requiring governance mechanisms to address vulnerabilities across multiple dimensions effectively.

In response, CSG for advanced nuclear power plants faces a unique set of challenges arising from the intricate interplay of technical, operational, and sociopolitical factors. One significant challenge lies in the technical complexity of future nuclear power plants. Such plants can be conceptualized as systems composed of interconnected physical, digital, and human components, each with distinct vulnerabilities. For example, cyber threats targeting control systems or data integrity can compromise operational safety and regulatory compliance (Williams, 2020). Similarly, physical security threats, such as sabotage or unauthorized access, require robust defense mechanisms that integrate seamlessly with primary operational priorities. Governance frameworks must, therefore, coordinate between these diverse functional perspectives to maintain resilient nuclear power plant operations. Specifically, advanced nuclear power plants will consist of novel operational systems, including new nuclear material forms, fuel handling processes, reactor technologies, and ancillary support mechanisms that differ significantly from traditional nuclear reactors. This shift both requires a thorough understanding of the range of operational effects of such changes and the evolution of bespoke resilience (and security) measures adequate to effectively mitigate newly emerging associated risks.

Yet, operational unpredictability further complicates governance. For example, while routine nuclear power plant operations may align with the "simple" or "complicated" domains of the Cynefin framework, unexpected disruptions—ranging from equipment failures to natural disasters—can rapidly shift the environment into the "complex" or "chaotic" domains. The system's governance must adapt dynamically to these shifts, employing strategies that balance immediate response with long-term system stability. Here, the potential for remote, urban, or temporary deployment of advanced nuclear power plants raise additional concerns for operational resilience and security. The complexity and uncertainty introduced by the flexibility of advanced nuclear power plants could result in deployment to locations where personnel may lack extensive experience in nuclear operations and facility resilience.

Another critical challenge involves the sociopolitical context in which nuclear power plants operate. Regulatory frameworks, international oversight, and public perceptions of nuclear energy all exert influence on governance strategies (Bowen et al., 2024). Navigating these external pressures requires a governance system that is not only compliant with stringent regulations but also agile enough to address evolving political and societal expectations. Additionally, the global nature of nuclear oversight necessitates harmonization of governance practices across different jurisdictions, which often have varying priorities and standards. More specifically, national regulatory uncertainty and fledgling international guidance for deploying advanced nuclear power plants may lead to situations where operations, safety standards, and security protocols not sufficiently robust or appropriate.

In addition, these challenges faced by advanced nuclear power plants are substantially impacted by a constantly evolving threat landscape. Consider the previously mentioned anticipated increase in digitization for these advanced nuclear systems. In addition to increased operational efficiency, more digitization and automation also expands cyber and physical attack surfaces, thus creating new vulnerabilities susceptible to potential manipulation. Similarly, wider deployment to needy regions indicates advanced nuclear power plants may be located closer in proximity to a wide array of malicious non-state actors. As the capabilities of such malicious groups improve, the broader deployment of advanced nuclear power plants to remote areas potentially allows more opportunities for sophisticated adversary actions. Lastly, there is noticeable shift in advanced nuclear power plant design related to security, trading the (more costly) tradition of adding “layers” for passive safety to increase security performance. This transformation underscores the benefit of a systems governance approach to incorporate systems security into operational resilience to better mitigate the complexities of modern threats.

By addressing these multifaceted challenges (summarized in Table 2., below), governance frameworks can enhance the security—and, therefore, the resilient operations—of advanced nuclear power plants. Therefore, the Cynefin domains for advanced nuclear power plants may manifest as operational routines (simple), intricate technical systems (complicated), dynamic interactions (complex), and unexpected crises (chaotic) in remote, urban, or temporary operational environments with no previous experience with nuclear energy. More specifically, a systems governance-based approach leverages insights from systems theory and security heuristics to develop adaptive and holistic strategies for resilient operations in each of these domains.

Table 2 Summary of major challenges and corresponding governance/security responses required for resilient operations of advanced nuclear power plants

Challenge Area	Key Drivers / Features	Implications for Resilience	Governance / Security Response (CSG)
Technical Complexity	Passive safety systems, new materials, reactor designs, digitization, automation	New vulnerabilities; interdependent subsystems; expanded cyber-physical threat surface	Integrated security architecture; resilience-by-design; coordination across physical, digital, and human systems
Operational Unpredictability	Remote or mobile deployment; temporary sites; inexperienced personnel; dynamic environments	Increased risk of domain shifts (from simple to chaotic); limited local response capacity	Adaptive governance frameworks; real-time monitoring; dynamic role and responsibility assignment based on Cynefin domains
Sociopolitical Uncertainty	Regulatory inconsistency; evolving international standards; public perception and acceptance	Potential misalignment between safety/security standards and operational needs	Agile, multi-jurisdictional governance; transparent communication; regulatory harmonization; scenario-based planning
Evolving Threat Landscape	Advanced adversaries; proximity to non-state actors; trade-off of layered security for cost-efficient passive systems	Increased threat sophistication; security assumptions may no longer hold	Systems security as a governance function; feedback-enhanced situational awareness; multi-layered detection and response mechanisms

Conclusions & Implications

CSG offers a rigorous, logical, and comprehensive approach for incorporating security more intimately into system persistence, adaptation, and transformation. Leveraging core systems theoretic tenets (e.g., feedback processes and circular causality) and insights from current systems models (e.g., the Cynefin framework), governance-based approaches can incorporate security into operational resilience in environments characterized by uncertainty, interdependence, and high consequences. Here, the anticipated dynamics and trends associated with advanced nuclear power plants exemplify such environments. In response to the inherent focus on responding to disruptions, CSG can help mitigate the complexity introduced by new intrinsic (e.g., new reactor technologies and novel nuclear fuel types) and extrinsic (e.g., remote operating environments and increased digital communications) deployment issues associated with advanced nuclear power plants.

By invoking metasystem functions, CSG provides control, communication, coordination, and integration for resilient system operations across domains, including operational routines (simple), intricate technical systems (complicated), dynamic interactions (complex), and unexpected crises (chaotic). From this perspective, CSG models provide credible pathways for incorporating systems security among difficult cross-dimension interactions between

technological complexity, the role(s) of human actors, and non-linear operational environments. Though this article focused on security for nuclear power plants, the underlying logic supports current efforts in the INCOSE systems security engineering community to shift towards an emphasis on ensuring functional persistence of the system in predatory, contested environments. By extension, CSG also affords the opportunity to optimize persistence, adaptation, and transformation efforts to mitigate real-world complexities, dynamic challenges, and disruptive technologies acting against operational system resilience. Advocating for security as an integral part of the system's governance provides insights for enhancing resilient system operations in complex and chaotic environments.

References

Bowen, W.Q., Cottee, M., Tzinieris, S., 2024. The Evolution of Global Nuclear Security Governance, in: Hobbs, C., Tzinieris, S., Aghara, S.K. (Eds.), The Oxford Handbook of Nuclear Security. Oxford University Press, p. 0. https://doi.org/10.1093/oxfordhb/9780192847935.013.11

Caskey, S., 2024. A Theoretical Framework For Resilience In Complex System Governance (CSG) (Dissertation). Old Dominion University, Norfolk, VA.

Castelle, K., Bradley, J., Baugh, D., suffix, C., 2015. Systems theory as a foundation for governance of complex systems. Int. J. Syst. Syst. Eng. 6, 15–32. https://doi.org/10.1504/IJSSE.2015.068805

Cook, R., 2002. How complex systems fail.

Keating, C.B., Bradley, J.M., 2015. Complex system governance reference model. Int. J. Syst. Syst. Eng. 6, 33. https://doi.org/10.1504/IJSSE.2015.068811

Keating, C.B., Katina, P.F., 2023. Complex System Governance: Theory and Practice. Springer.

Keating, C.B., Katina, P.F., Pyne, J.C., Sisti, J.A., Gheorghe, A.V., 2022. Coupling quantitative vulnerability assessment and complex system governance for systems of systems. Int. J. Syst. Syst. Eng. 12, 114–133. https://doi.org/10.1504/ijsse.2022.124979

Ross, R., Winstead, M., McEvilley, M., 2022. Engineering Trustworthy Secure Systems (No. NIST Special Publication (SP) 800-160 Vol. 1 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v1r1

Snowden, D., 2017. Liminal Cynefin. Cynefin Co. URL https://thecynefin.co/liminal-cynefin/ (accessed 12.19.24).

Snowden, D., Boone, M., 2007. A Leader's Framework for Decision Making [WWW Document]. URL https://hbr.org/2007/11/a-leaders-framework-for-decision-making (accessed 10.9.24).

Williams, A., Caskey, S., 2024. Building a Scientific Foundation for Security: Multilayer Network Model Insights for System Security Engineering. INCOSE Int. Symp. 34, 224–238. https://doi.org/10.1002/iis2.13143

Williams, A.D., 2020. Systems Theory Principles and Complex Systems Engineering Concepts for Protection and Resilience in Critical Infrastructure: Lessons from the Nuclear Sector. INSIGHT 23, 14–20. https://doi.org/10.1002/inst.12293

Author Bios

Dr. Sue Caskey is an adjunct professor in System of Systems (SoS) Engineering at Old Dominion University (ODU). She is a research and systems analyst at Sandia National Laboratories with nearly 30 years of international security expertise. A founding member of Sandia's Global Chemical and Biological Security program, she has supported physical and procedural security assessments and improvements in over 30 countries. Dr. Caskey currently leads analytical projects on global threat prioritization and risk assessment across the chemical, biological, radiological, and nuclear (CBRN) domain—including emerging technologies. Her work supports U.S. Department of State, Department of Energy, and Department of Defense cooperative threat reduction efforts, developing novel tools and models to address current and emerging threats. She also founded a cross-cutting working group at Sandia focused on global analysis and data management. She holds M.E. and Ph.D. degrees in Systems Engineering from ODU and dual B.S. degrees in Biology and Computer Science from the University of New Mexico. Active in IEEE, INCOSE, and the Society for Risk Analysis, she continues to contribute to the academic and professional systems community.

Dr. Adam Williams is a subject matter expert (SME) on cyber-physical nuclear systems, complex risk for national security issues, and innovative solutions to uncertain global security challenges. Currently, he serves as the Global Security Strategic Studies lead for Sandia's Cooperative Monitoring Center, leads the development of Sandia's Global Security University, provides strategic technical support for various U.S. sponsors (and R&D projects), and is the Nuclear Security & Physical Protection Technical Division chair for the Institute of Nuclear Materials Management (INMM). Dr. Williams also leads and serves as an SME on U.S. Department of Energy's National Nuclear Security Administration (NNSA), Laboratory Directed Research and Development, Electric Power Research Institute, and Department of State (DOS) initiatives. Dr. Williams has a Ph.D. in Engineering Systems, Human-Systems Engineering from the Massachusetts Institute of Technology (2018). He also has an M.A. in International Affairs from the George Bush School of Government & Public Service (2007) and a B.S. in Mechanical Engineering (magna cum laude, 2004) from Texas A&M University.