SAND2019-6455C

Socio-Technical Interactions: A New Paradigm for Nuclear Security

Adam D. Williams

Sandia National Laboratories, Albuquerque, NM, USA, adwilli@sandia.gov*

Traditional physical protection system (PPS) design approaches (e.g., the renowned Design Evaluation and Process Outline-DEPO) tend to generate the same PPS design—and estimate for PPS effectiveness—for a given nuclear facility before and after a significant shift in corporate culture, operational priorities, or personnel turnover. On the other hand, the International Atomic Energy Agency (IAEA) offers a nuclear security culture model that uses a combination of management systems, leadership behaviors, and personnel behaviors to explain this potential variance in security performance stemming from social—rather than technical—changes. This disconnect suggests the need for a way to reconcile how the same nuclear facility can have different levels of security performance.

The nuclear security, nuclear safety, organization science, and engineering systems literatures offer insights for explaining this disconnect. Some of these insights indicate that patterns of security practice are key drivers for understanding security performance—but are not adequately addressed in common security analysis approaches. Other insights illustrate the importance of how technical (e.g., PPS) and social (e.g., nuclear security culture) systems interact in explaining security performance. Still other insights suggest that an engineering systems approach is helpful in understanding how such socio-technical interactions and patterns of behaviors affect security performance levels.

In support of these insights, this paper introduces a 2x2 matrix that provides a way to organize the relationships between PPS adequacy, security operations, adherence to procedures, and security performance to reconcile this disconnect in current approaches to nuclear security analysis. Though seemingly a static classification scheme, this socio-technical model for nuclear security introduces the importance of dynamic changes as drivers of security performance. After explaining this socio-technical model for security, this paper will discuss how security for nuclear facilities can be described in terms of interactions between technical (e.g., DEPO-based PPS) and social, or non-technical' (e.g., IAEA nuclear security culture model-based) elements. Lastly, this paper will discuss implications for how this new paradigm can foster improvements for understanding, designing, operating, and evaluating nuclear security.

INTRODUCTION[1]

Traditional physical protection system (PPS) design approaches (e.g., the renowned Design Evaluation and Process Outline-DEPO [2]) tend to generate the same PPS design—and estimate for PPS effectiveness—for a given nuclear facility before and after a significant shift in corporate culture, operational priorities, or personnel turnover. On the other hand, the International Atomic Energy Agency (IAEA) offers a nuclear security culture model that uses a combination of management systems, leadership behaviors, and personnel behaviors to explain this potential variance in security performance stemming from social—rather than technical—changes. This

[1] This conference paper summarizes one of the key analytical arguments of [1].

* **SAND2010-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.

disconnect suggests the need for a way to reconcile how the same nuclear facility can have different levels of security performance.

Consider, for example, an anecdote from a former NNSA Chief of Defense Nuclear Security[2] recounting the 1983 transition in organizational ownership of security at Savannah River Site:

> In his time at Savannah River Site there was a distinct difference in security performance between when DuPont and Wackenhut held responsibility for site security. With each providing sufficient levels of preparation for security personnel, the overly cautious/ occupational safety conscious culture of the former (e.g., insufficient commitment) severely limited the success of response to security events—especially when compared to the action and accountability-oriented philosophy, and resultant strong performance, of the latter. During the Dupont tenure at Savannah River Site, there were few security incidents (but a highly cautious M&O contractor who had responsibility for security). For example, during a security force training course on hostage rescue (recapturing a reactor control room from adversaries), when it was time to dispatch the special response tam, the security managers would not do so, on the argument that it was too dangerous (per the DuPont risk-averse/safety corporate culture). After the change to Wackenhut, as a specific security contractor a few years later, there was a change in security operations philosophy, one of more action and accountability. For example, shortly after this change, there was a night time perimeter fence alarm near one of the reactors. The security personnel scrammed the reactor, removed the operators, called the SRT and local law enforcement and then conducted an "inch-by-inch search" of the facility. And, "Though we never found anything…the serious response was a great experience."

Here, the shift from a *risk-averse, safety corporate culture* to an emphasis on *action and accountability* influenced security practices and resulted in more timely and enthusiastic responses to physical protection system (PPS) alarms. According to this anecdote, security performance at Savannah River Site improved *without* any significant changes to the PPS.

Yet, DEPO-based approaches would generate the same PPS design and estimate for PPS effectiveness for the facility before and after the transition. Despite the same PPS being in place, Interviewee P indicated a difference in the resultant security performance missed by this class of approaches. On the other hand, the IAEA offers a nuclear security culture model that uses a combination of management systems, leadership behaviors and personnel behaviors to explain this variance in security performance after the security ownership transition described by Interviewee P. Though a helpful step, nuclear security culture-based approaches do not clearly relate these desired characteristics to security performance measures. These limitations in current approaches to nuclear

[2] This is interviewee P from [1].

security suggest the need for a way to reconcile how the same nuclear facility with two different operators can have different levels of security performance.

INSIGHTS FROM A MULTIDISCIPLINE LITERATURE REVIEW

Overall, the traditional focus on technological solutions (like in DEPO) seems based on the implicit assumption that any task necessary for the PPS to achieve desired levels of performance will be completed adequately and with high quality. This is a simplifying and untenable assumption at the core of DEPO-based approaches that negates the impacts of non-technical influences on security performance. Some extensions to DEPO demonstrate that such non-technical influences can be modeled as influences on control over PPS components [3] or in terms of organizational influences on accomplishing PPS functions [4]. Yet, these approaches still struggle to fully reconcile with the common refrain from former U.S. Department of Energy security czar (and former commander of U.S. strategic forces) General Eugene Habiger that "good security is 20 percent equipment and 80 percent culture."[5]

If "good security" is "80% culture," then there is a stark need to better understand—and incorporate—the role of human and organizational behaviors in nuclear security. Efforts to explain the influence of such human and organizational behaviors on nuclear security performance include a range of approaches developed across a spectrum of nuclear security-related stakeholders. For example, [6] offers a non-academic interview study that describes how individual perceptions (e.g., under-trained, and underpaid guards) and organizational decisions (e.g., low priority for security) negatively impact nuclear security performance. Another effort, by Los Alamos National Laboratory, adapted safety human error analysis to evaluate actions comprising and conditions related to over 100 security incidents related to classified information taking place between 1999 and 2001.[7] Yet another to address the human factor in security from the DOE national laboratory complex is based on the idea of security climate—which highlights the importance of "employees' shared perceptions of the organization's security policies, practices, and procedures" [8, p. 102], as an explanatory concept that addresses the human factor in nuclear security. Despite the useful insights drawn from these efforts, none of them provide a way to better incorporate human and organizational behaviors into security performance analysis.

In response, insights from organization science can also help address the influence of human and organizational behaviors on nuclear security performance. This academic discipline explores how individuals construct institutions, processes and practices to achieve a common goal. For example, [9] and [10] argue that differences between designed and as-built organizations can lead to unexpected outcomes—which suggests that understanding the relationship between daily work practices (as-built) and performance assumptions (design) can help better explain these human/organizational influences. Another argument states that it is useful to investigate such organizational behaviors from three distinct perspectives: the strategic design lens, political lens and cultural lens.[11] The three lens approach suggests that performance assumptions underlying PPS designs are influenced by both the independent focal areas of and the interactions between each lens. If [11] argues that working across the three lenses offers a more comprehensive understanding of organizational behavior, then it may be useful to describe the operational context in which PPS operates in terms of the dynamics between each lens.

The Structurational Model of Technology (SMOT) serves as an instructive example of such an approach.[12] SMOT offers a recursive description of how human agent actions situate the uses of

technology, which then shapes the enacted organizational structure that produces institutional properties that enable or constrain those human agent actions. By replacing technology with PPS, the common understanding of nuclear security gives way to perceiving security performance as human agents interacting with the PPS under the influences of institutional properties. Ultimately, these institutional properties affect the actions of the human agent—indicating that organizational influences can reinforce or oppose human agent activities (and therefore security system performance). The logic of SMOT offers two useful insights for describing the relationship between PPS and human/organizational behaviors. First, the structuration perspective indicates the importance of daily work behaviors and how patterns of behavior change organizational structure and outcomes. Second, where works tasks require the use of technology, their execution emerges from the interaction(s) of those technologies, human agents and institutional properties. This perspective describes nuclear security as recursively completing work tasks as human agents are influenced by the interaction of selected PPS technologies.

Engineering systems—a growing academic discipline seeking to develop theory and practice in characterizing and analyzing complex causality and system behaviors in their socio-political contexts—offers a new paradigm for incorporating these insights from organization science. According to the key characteristics established in [13], engineering systems offer a way to reconcile these insights to explain nuclear security performance as "characterized by a high degree of technical complexity, social intricacy, and elaborate processes, aimed at fulfilling important functions in society." [13, p. 31] An engineering systems approach provides a strong theoretical basis on which to explore nuclear security performance as a result of the interdependence between PPS and human/organizational behaviors. For example, this perspective supports the argument that security performance is the result of technical PPS capability and individual daily work practices. Further, this logic suggests that these individual work practices can be described in terms of specific tasks (elicited from system design) necessary to achieve desired levels of security performance. If completing nuclear security tasks is dependent upon the validity of assumptions on how the PPS will be used, an engineering systems perspective then suggests these assumptions can be reframed as performance requirements on individual security behaviors. And, according to organization science, these individual work practices are also influenced by institutional properties and organizational pressures. This explicitly addresses the limitation in DEPO-based approaches where these tasks are assumed to be completed with high quality.

In this way, an engineering systems approach also seems able to illustrate how insights from a multidiscipline literature review helps better describe the interactions of technical PPS design and human/organizational behaviors. These new insights establish a foundation for constructing such a holistic and interdisciplinary approach to nuclear security performance. Organization science introduces the insight that the size of the gap between expected and actual operations affects overall performance—including a description of recursive relationships between security technologies and human, social and organizational factors. Based on successful experiences in engineering systems analysis for a limited set of security-related applications, such a perspective seems better suited for overcoming the challenges faced by current approaches to better address the PPS and human/organizational behavior interdependencies. As such, shifting the perspective toward understanding nuclear security performance as emerging from the interactions between technologies, organizational influences and personnel seems better suited for explaining human/influences on nuclear security performance. More pointedly, when describing the difficulties surrounding the successful implementation of nuclear security culture, one expert noted the

> importance of interaction among designers, operators, and overseers or regulators…Today, systems are not just technical, but sociotechnical; technical systems are as important as the people who operate them. [14, p. 39]

Motivation: The Need for a New Approach to Nuclear Security

Arguments across literatures and insights from my empirical studies motivated the exploration of an engineering systems approach to nuclear security. Professional experience and observations suggest that the patterns of security practice observed in the empirical data can be described from two perspectives. In the first perspective, patterns of security practice are described in relation to *expected behaviors* of security personnel as they interact with the PPS to achieve overall performance goals. This perspective—often held by PPS designers, PPS engineers, and operations managers at nuclear facilities—tends to evaluate success in terms of how well security-related behaviors align with *the letter of the procedure*. Conversely, in the second perspective, patterns of security practice are described in relation to *actual behaviors* of security personnel as they interact with the PPS to achieve overall performance goals. This perspective, often held by security personnel, first-line security managers and PPS installers, tends to evaluate success in terms of how well security-related behaviors support security functions. Current state-of-the-art nuclear security analysis approaches, based on this first perspective, are logically founded on two key assumptions: (1) adequate PPS security procedures exists to support PPS operations and (2) strong security performance occurs when the *actual* security behaviors align with the *expected* security behaviors (often expressed in terms of adhering to established procedures).

An engineering systems approach is helpful in understanding how different interdependencies and security performance levels result when these assumptions are relaxed or challenged. Figure 1, below, shows a 2x2 matrix that illustrates the relationship between PPS adequacy, the alignment between actual and expected security behaviors, levels of adherence to security procedures and security performance outcomes.

	Actual security operations = Expected security operations	***Actual security operations ≠ Expected security operations***
Adequate PPS Design (~P_E)	Adequate security procedures Strict adherence to related procedures **STRONG Performance** **(A)**	Adequate security procedures Deficient adherence to related procedures **WEAK Performance** **(B)**
Inadequate PPS Design (~P_E)	Inadequate security procedures Strict adherence to related procedures **WEAK Performance** **(C)**	Inadequate security procedures *"Going beyond" adherence to related procedures* **STRONG Performance** Inadequate security procedures *Deficient adherence to related procedures* **WEAKEST Performance** **(D)**

Figure 1. 2x2 Matrix of Logical Relationships Between PPS Design and Security Operations

In these terms, DEPO-based approaches focus on achieving strong security performance through technical PPS performance (the top row in Figure) and tend to assume strict adherence to adequate security procedures. Similarly, IAEA nuclear security culture model-based approaches encourage strict adherence to security procedures (the left-hand column in Figure) and tend to assume the existence of an adequate PPS. As such, these overlap in quadrant A of Figure —where adequate security procedures exist and facility personnel exhibit strict adherence—to produce strong performance. In many cases, these approaches argue that once achieved, security performance will remain in this state. By extension, current approaches describe weak performance in terms of an adequate PPS (and related procedures) combining with deficient adherence to those protocols (quadrant B). Quadrant B then clearly supports the argument that non-technical influences can cause the actual use of PPS to inadequately achieve desired levels of security performance.

While quadrants A and B are commonly accepted, what is not commonly accounted for are instances where strict adherence to security procedures (the alignment of actual and expected security behaviors) results in weak security performance (quadrant C). This non-traditional weak state further illustrates the benefit of conceptualizing security performance as the result of interactions between technical and non-technical security influences. More specifically, this quadrant identifies the limitations of efforts that solely emphasize personnel adherence to security protocols to achieve desired security performance levels. Likewise, current approaches do not clearly address the non-traditional strong performance resulting from personnel going *above and beyond* strict adherence to security procedures to compensate for inadequate PPS (one possibility in quadrant D). Here, examples of going *above and beyond* include security personnel bypassing procedures known to be deficient and ignoring procedures not related to achieving security functions. While there is no recipe for strong security performance that says "have an inadequate PPS design and encourage personnel to ignore procedures," this quadrant helps acknowledge the realities of security operations where personnel[3] sometimes need to not adhere to procedures to overcome gaps and challenges to the PPS design that can occur from time to time. While theoretically possible, this potential outcome is both extremely unlikely and describes a poorly designed PPS.

There is a second—and more commonly observed—interpretation that consists of security personnel with deficient adherence to security procedures and a poorly designed PPS. This situation results in the (conceptually) weakest possible security performance. It does seem likely that the same influences and factors that resulted in a poor PPS design would similarly result in inadequate adherence to related procedures. Avoiding this potential outcome is one of the major drivers behind many of the international efforts to bolster nuclear security. Whatever the likelihood of the two variants of Quadrant D, they reinforce the benefit of defining security performance as an emergent property of the interactions between technical system design and human/organizational behaviors.

Though seemingly a static classification scheme, this 2x2 matrix introduces the importance of dynamic changes in the drivers of security performance. For example, certain influences or behaviors *in the moment* that result in strong security performance may have longer-lasting, time-

[3] Evaluating the individual capability of security personnel in this regard was beyond the scope of [1] and could be the basis for future research.

delayed side effects on future security operations. Consider the example from a PPS design/installation manager for DOD and NNSA facilities[4] that describes how

> on three different occasions during a walk-down inspection of the mile-long perimeter intrusion, detection and assessment system at a military facility with nuclear assets, they were told, "Halt, on the ground"—despite having the necessary approvals and being a guest of the facility to inspect security upgrades. The security personnel were taught that, "Anything other than nothing going on is off-normal" and requires an immediate response—including up to a complete facility lockdown.

Although the security personnel showed strict adherence to adequate protocols (quadrant A) that resulted in strong security performance at the time—repetitively forcing inspectors to the ground wastes resources—undermines cooperation between inspectors and security personnel and contributes very little to overall security performance potentially leading eventually to quadrant B.

The framework illustrated in Figure 1 provides a way to organize the relationships between PPS adequacy, security operations, adherence to procedures and security performance to reconcile key assumptions in current approaches to nuclear security analysis and practical observations. Further, the extent to which levels of adherence to security protocols drive strong security performance determines the importance of identifying (ideally designable and controllable) influences on individual levels of adherence. Consistent with insights from the organization science and engineering systems literatures, security for nuclear facilities can be described in terms of interactions between technical (e.g., adequate PPS design) and social, or *non-technical*' (e.g., alignment between *actual* and *expected* operations) components. Building on core attributes of engineering systems [13], Figure 1 offers a new approach for explaining—and hopefully better managing—the interactions between PPS and human/organizational behaviors in nuclear security.

Though a useful reframing that addresses several shortcomings in current approaches, there is a need to further explore the dynamics that described the movement within the 2x2 matrix of security performance outcomes (Figure 1). Similar to the "migration toward the boundaries of acceptable behavior" [15], "normalization of deviance" [16], "drift into failure" [17] and "system migration toward states of higher risk" [18], it would be useful and practically helpful to represent movement around the performance outcomes in this matrix. For example, future efforts could determining how positive movement (e.g., from Quadrants B, C or D to Quadrant A in Figure 1) can be initiated and sustained. Or, well-known organizational concepts could be mapped to movement on the matrix—like mapping continuous improvement as movement between Quadrant A to the strong interpretation of Quadrant D (and back). Lastly, the possibility of identifying milestones (positive) or benchmarks (negative) to indicate movement could be explored to more fully leverage this new framing of nuclear security performance.

CONCLUSIONS

As suggested in this paper, an socio-technical systems approach offers several new insights for understanding nuclear security performance. First, this framework articulates that security performance is a system-level property that requires both technical reliability of the PPS (rows of the

[4] This is interviewee B from [1].

matrix in Figure 1) and behavioral quality of security personnel (alignment of *actual* and *expected* operations in the columns of Figure 1). This matrix also helps explain how different interactions between technical reliability and behavioral quality result in a range of security performance outcomes—including both traditional (quadrants A and B) and non-traditional (quadrants C and D) understandings of security outcomes shown in Figure 1. The former are supported by DEPO and IAEA nuclear security culture model-based approaches, while the latter expand beyond these traditional approaches to offer a higher fidelity explanation of nuclear security performance. This matrix also helps explain how different nuclear security stakeholders can have different definitions of success. For example, how PPS designers, PPS engineers and operations managers at nuclear facilities see quadrant A (in Figure 1) as a success, while security personnel, first-line security managers and PPS installers would also see the effective portion of quadrant D as successful. Similarly, organization scientists are likely to argue that quadrant A is impossible and quadrant D is more realistic, while security engineers are likely to argue that this quadrant is rarely achieved. The matrix in Figure 1 helps guide this discussion and coordinate potential analysis techniques (as detailed in [1] and summarized in [19]).

The utility of this matrix implies that security performance is not a static attribute of nuclear facilities indicates a need to shift from optimizing PPS designs toward equilibrating socio-technical security interactions toward desired levels of performance. Similarly, this supports the conceptual argument that technical systems can never be so well designed that following a comprehensive list of rules can achieve desired outcomes (quadrant A in Figure 1). Rather, nuclear security performance is best understood as individuals and organizations adjusting and compensating for inadequacies in the PPS design. This is consistent with "calls for continuous improvement" [20] from nuclear security experts and the engineering systems argument that security is an emergent—and dynamically changing—property of nuclear facilities [1][19][21]. Ultimately, implementing this socio-technical systems framing establishes a new foundation for designing, operating, and evaluating nuclear security capable of incorporating *both* technical and non-technical elements to better combat 21st century threats.

REFERENCES

[1] Williams, A. (2018). Beyond Gates, Guards & Guns: The Systems-Theoretic Framework for Security at Nuclear Facilities. *PhD Dissertation.* Massachussets Institute of Technology.

[2] Garcia, M.L. (2008). *The Design and Evaluation of Physical Protection Systems (2nd Ed.).* Butterworth-Heineman.

[3] Nunes-Vaz, R., & Lord, S. (2014). Designing physical security for complex infrastructures. International *Journal of Critical Infrastructure Protection*, 7, 178-192.

[4] Argenti, F., Landucci, G., Cozzani, V., & Reneirs, G. (2017). A study on the performance assessment of anti-terrorism physical protection systems in chemical plants. *Safety Science*, 94, 181-196.

[5] World Institute for Nuclear Security (2016). *Nuclear Security Culture: WINS International Best Practice Guide, Rev. 3*. Vienna: WINS.

[6] Stockton, P. (2002). *Nuclear Power Plant Security: Voices from Inside the Fence.* Project on Government Oversight. Retrieved March 24, 2016, from http://www.pogo.org/our-work/reports/2002/nss-npp-20020912.html

[7] Pond, D. J. (2003). *Using Safety Tools to Improve Security, LA-UR-03-2381*. Los Alamos National Laboratory.

[8] Bitzer III, E. G. (2010). An Exploratory Investigation of Organizational Security Climate in a Highly Regulated Environment. *PhD Dissertation*. Colorado State University.

[9] Argyis, C. (1976). Single-Loop and Double-Loop Models in Research on Decision Making. *Administrative Science Quarterly*, 21(3), 363-375.

[10] Cyert, R., & March, J. (1963). *A Behavioral Theory of the Firm*. Englewood Cliffs, NJ: Prentice-Hall.

[11] Carroll, J. S. (2006). *Introduction to Organizational Analysis: The Three Lenses*. Cambridge, MA: Unpublished Manuscript.

[12] Orlikowski, W. J. (1992). The Duality of Technology: Rethinking the Concept of Technology in Organizations. *Organization Science*, 3(3), 398-427.

[13] de Weck, O., Roos, D., & Magee, C. (2011). *Engineering Systems: Meeting Needs in a Complex Technical World*. Cambridge, MA: The MIT Press.

[14] National Academy of Sciences. (2015). Brazil-U.S. Workshop on Strengthening the Culture of Nuclear Safety and Security: Summary of a Workshop. Washington, DC: The National Academies Press.

[15] Rasmussen, J. (1997). Risk Management in a Dynamic Society: A Modelling Problem. *Safety Science, 27*(2/3), 183-213.

[16] Vaughan, D. (1996). *The Challenger Launch Decision: Risky Technology, Culture and Deviance at NASA*. Chicago: University of Chicago Press.

[17] Dekker, S. (2011). *Drift into Failure: From Hunting Broken Components to Understanding Complex Systems*. Farnham, England: Ashgate Publishing Limited.

[18] Leveson, N. (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge, MA: MIT Press.

[19] Williams, A.D. (2018). "New Thoughts on Protecting Nuclear Materials and Facilities: A Systems-Theoretic Framework for Security," in *Proceedings of the 59th INMM Annual Meeting*, Baltimore, MD.

[20] International Atomic Energy Agency. (2014). *Information Circular: Communication Received from the Netherlands Concerning the Strengthening of Nuclear Security Implementation (INFCIRC/869)*. Vienna: International Atomic Energy Agency.

[21] Williams, A. D. (2013). System Security: Rethinking Security for Facilities with Nuclear Materials. *Transactions of the American Nuclear Society*, 109 (1), p. 1946-1947.