Chapter 3

The Importance of Context in Advanced Systems Engineering

Adam D. Williams*

Synopsis

Traditionally, systems engineering is predicated on a well-defined, mutually agreed upon operational environment. This perspective assumes a clear boundary between the interacting set of components of interest, precise definitions of external interfaces, known data limits, and anticipated patterns of use. Yet, the wave of change associated with the *Fourth Industrial Revolution* directly challenges these assumptions on how engineered systems will operate. In this chapter, we describe the traditional view of "context" in systems engineering and identify challenges to this view related to "Industry 4.0". We then offer insights from systems theory and organization science to address the blurring of the lines between "system" and "environment." The resulting idea of "context of use," the interrelated technological, environmental, social, and operational conditions by which system behaviors can be fully understood, is described and situated as an important element of advanced systems engineering. We conclude with a representative context of use example, a discussion of implications, and conclusions.

3.1 Introduction to Context for Advanced Systems Engineering

Systems engineering is predicated on understanding the interactions between components working toward a common goal. Traditionally, this perspective assumes a clear boundary between interacting sets of components, precise definitions of external interfaces, and known data limits to establish a well-defined, mutually agreed upon description of the conditions, settings, and circumstances in which systems are expected to operate. Oftentimes, these clear boundary definitions lead to a perception of the "environment" and the system's stakeholders as unidirectional, exogenous forces on the interactions within the system. This understanding assumes that system engineers' expectations of human behaviour perfectly align with how systems are *actually used*. Yet, this perspective fails to account for the role of human, social, and organizational influences on system behaviour. Moreover, this perspective cannot account for legacy effects (e.g., the difficulty of using digital replacement parts in analog nuclear power plant safety systems (National Research Council, Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, 1997)), historical memories (e.g., recollections of Challenger and Columbia on current NASA projects (Hall, 2003)), or long-standing assumptions about how the world works (e.g., Moore's Law of computational power evolution (Waldrop, 2016)) on interactions within systems. In short, "although traditional systems engineering does not completely ignore context influences on systems problem formulation, analysis, and resolution, it places context in the background" (Keating, *et al.*, 2003, p. 38).

*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. **SAND-PEER REVIEW.**

A traditional conception of environment in systems engineering fails to explain how "identical technologies [or systems] can occasion similar dynamics and yet lead to different structural outcomes" (Barley, 1986, p. 105) or "why different groups enact different…interaction(s) with a particular set of technological properties, in similar and different contexts" (Orlikowski, 2000, p. 420). The inability to explain how the *same* system employed in *similar* environments results in *different* performance outcomes suggests a limitation in traditional systems engineering approaches. This limitation, combined with the wave of technological changes associated with *Industrial Revolution 4.0*, suggests that traditional perspectives are insufficient for advanced systems engineering. Big data, emerging technology, and increasingly complex systems will likely result in the blurring of lines between use environments and system boundaries, changing roles of (and interactions with) stakeholders, and increasing variability in human behaviours in system use. For example, in comparing the different outcomes of implementing the same information management system at two extremely similar companies, Robey and Rodriquez-Diaz (1989) argued that

> The social context of [system] implementation includes the specific organizational setting which is the target of the implementation and the wider cultural and national setting within which the organization operates. (p.230)

This outcome demonstrates the need to better undertand—and account for—the importance of *context* in systems engineering.

In approaching "advanced systems engineering," there is a need to relax traditional assumptions of boundary clarity, exogenous influences, unidirectional requirements, and environment-independent definitions of risk or success. This is especially salient as operating environments and stakeholders move from simply being exogenous forces *on* a system to being constituent parts *within* a system of systems. Here, perhaps the "novelty" of novel technologies is how they challenge traditional assumptions of the context in which systems operate. Taking insights from systems theory, organization science, and engineering systems results in an emphasis on the "context of use"—the conditions, settings, and circumstances in which systems operate—for advanced systems. Context of use, consistent with the "worldview" perspective offered by the INCOSE fellows (Silitto, *et al.*, 2018), is defined as the conditions, settings, and circumstances in which systems operate. Including context of use in advanced systems engineering can help to navigate the challenges posed by the *Industrial Revolution 4.0*. After reviewing perspectives of context in traditional systems engineering, this chapter explores gaps in traditional views, introduces non-traditional approaches to context for systems, and provides more detail on the "context of use" concept for advanced systems engineering. The chapter ends with a representative context of use example using physical security systems for high consequence facilities, a discussion of implications, and conclusions.

3.2 Traditional View(s) of Context in Systems Engineering

Context is defined by Meriam-Webster's Dictionary as "the interrelated conditions in which something exists or occurs," while the Oxford Dictionary defines it as "the circumstances that form the setting for an event, statement, or idea, and in terms of which it can be fully understood." For systems engineering, conditions, settings, and circumstances are often defined by establishing boundaries that separate the set(s) of interrelated components of concern from their environment. While such boundaries consist of physical (or digital) limitations (e.g., property borders of a

*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. **SAND-PEER REVIEW.**

manufacturing facility or restrictions on computing power), they also include perceptions of performance requirements, stakeholder involvement, and functional outcomes. This concept is evident in how the official INCOSE definition for systems engineering focuses

> …on defining customer needs and required functionality…[that] considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs.

Establishing system boundaries to describe the conditions, settings, and circumstances for system operations has provided a common and useful framework for improving system design and performance. Organizing systems analytical and implementation thinking around component behavior requirements and performance outcomes has allowed systems engineering to advance the state-of-the-art solutions provided to customers across a range of professional domains. This approach, which is common across engineering disciplines, leverages a "value-free" engineering paradigm where the "focus is almost wholly on the abstract concepts, principles, and methods of the domain" (Bucciarelli, 2010, p. 10). In this paradigm, stakeholders are considered exogenous forces on an open system or assumed out of a closed system.

Systems engineering also includes assumptions of the ability to *control* system boundaries. For example, in one clear example of traditional view(s) of context, Kenett, *et al.* (2018) identified that current systems engineering typically depends

> on that fact that the assumption that the system had a stable, well-constructed set of requirements, a well-defined and manageable set of stakeholders and their expectations, and well-known and controllable constraints on and boundaries of the system. (p. 1609)

From this perspective, defining conditions, settings, and circumstances for systems engineering is an exercise in clearly articulating what a system has control over (e.g., "stable," "well-constructed," "well-defined," "manageable," or "well-known") and what it does not (e.g., everything else). In many ways, focusing on identifying and developing such crisp, clear, and controllable aspects of a system boundary results in a deeper understanding of the range of potential behaviors that can emerge from component interactions. When variability in a system boundary arises, efforts are focused on reducing (or removing) the associated uncertainty by changing performance requirements or adjusting the limits on component behaviors. While there are numerous advantages to using "open system" or "closed system" principles, solely relying on these approaches is insufficient to adequately account for the technological changes associated with *Industrial Revolution 4.0.*

3.3 Challenges to Traditional View(s) of Context in Industrial Revolution 4.0

As discussed in earlier chapters of this book, several aspects of *Industrial Revolution 4.0*, such as big data, emerging technologies, and increasingly complex systems, are driving a need to evolve toward advanced systems engineering. Yet, these drivers also directly challenge assumptions in traditional systems engineering on the ability to control the conditions, settings, and circumstances in which increasingly complex systems must operate. Consider the impact of "big data" on vehicle manufacturing systems. Current manufacturing systems define their operating context in terms of individual purchasing histories, geographical purchasing patterns, and vehicle-specific sale trend data

*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. **SAND-PEER REVIEW.**

streams. Here, purchasing dynamics act as unidirectional signals to trigger changes in manufacturing system performance outputs—for example, production of electrical cars may increase in response to new, more restrictive emissions regulations. Big data, however, can couple these traditional data streams with new, non-traditional data to help forecast modifications in manufacturing necessary to meet, and perhaps even *change*, customer needs. Incorporating non-traditional data such as trends in public transportation usage and changes in average distances between homes and places of employment can improve the efficiency and effectiveness of vehicle manufacturing systems meeting customer needs. In addition, vehicle manufacturing systems—by producing *more* electrical vehicles—can in turn *influence* the operating environment by increasing societal support of more restrictive emissions regulations. By affording opportunities to influence a system's operating environment, "big data" challenges the efficacy of traditional systems engineering views of context.

Consider autonomous vehicles as an example of emerging technology that challenges conventional systems engineering approaches to context. The systems engineering assumptions on controlling data presented to automobile drivers in the 1990s are insufficient to provide the same system-level performance in today's artificial intelligence-based vehicles. Vehicles developed in the 1990s provided a limited amount (and type) of data to the human driver about vehicle performance. Data taken in by the vehicle was similarly limited. Systems engineers could define operating conditions, settings, and circumstances based on the human driver as the components of the vehicle interacted to provide transportation and responded to the exogenous influences of the driver on component interactions (e.g., braking). These same assumptions that humans act as the boundary between the vehicle and the environment are inadequate for developing autonomous vehicles. These vehicles require an immense amount of data types to flow *between* the vehicle and the driving environment. For example, emergency braking or lane correction technologies send signals out to identify other vehicles or the road itself and receive data on which to make driving decisions. As autonomous vehicles direct components to change their individual and interdependent behaviors to move the vehicle, the movement changes the environment in which the vehicle operates. The ability for emerging technologies to affect dynamic change in their operating environments challenges traditional unidirectional perceptions of context.

Increasingly complex systems pose the clearest challenge to traditional systems engineering perspectives on context. One approach to addressing increasing complexity is a *system-of-systems* (SOS) approach where isolated systems are interpreted as interacting components of metasystems to achieve desired goals. Keating, *et al*., (2003) argue that this perspective "dictate[s] increasing appreciation for contextual influence on all aspects" of SOS and further assert that "assumptions based on stability in…contextual domains must be considered suspect in SE" (p. 41). A similar approach to addressing system complexity argues that "actualizing the engineered [system] solutions…within the real system…[involves] working with decision makers (change the world), other researchers (change the field) and people affected by the change (understand the impact)…through a [system] solution's lifecycle" (Glass, *et al*., 2012, p. 12). Developed at Sandia National Laboratories, this *complex, adaptive systems of systems* (CASoS) engineering approach adopts a wider view of systems engineering by shifting away from "[technological system] solutions that assume isolation (at smaller scales)" because complexity stems from socio-economic-ecologic-technical "feedbacks from outside the (narrowly) idealized system" (Glass, *et al*. 2012, p. 14). For these two approaches, increased complexity is addressed by relaxing rigid system boundary definitions and including more external interactions with other systems.

*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. **SAND-PEER REVIEW.**

Rather than calculating complexity by looking at the interplay between systems, the *complex, large-scale, interconnected, open system* (CLIOS) perspective defines systems as "consisting of a physical domain embedded (conceptually) in an institutional sphere" (Sussman, 2014, p. 13). With CLIOS, complexity is partially addressed by "explicitly includ[ing] the institutional world as part of the system" (Sussman, 2014, p. 13) and acknowledging that changes in these institutional worlds can drive both enhanced system performance and unwanted system behaviors. Different approaches toward capturing increasing complexity in systems represent common characteristics that gave rise to a new academic discipline at the Massachusetts Institute of Technology called *engineering systems*. This perspective addresses increasing system complexity by the linking of "technological artifacts, enabling networks, the natural enivonment, and human agents" (de Weck, *et al*. 2011, p. 15). De Weck, *et al*. (2011) also characterized engineering systems by how the "configuration of the entire system—its properties, elements, and interrelationships—are always fluid, always changing with time" (p. 37), allowing for a bi-directional relationship between technological systems and human use(s) of those systems.

Each of these approaches to increased system complexity—which is only expected to increase *further* in the *Fourth Industrial Revolution*—establish that "both the technical aspects and the social context within which the systems are operating play a central role" (Sussman, 2014, p. 7). This demonstrates the need to address changes in how systems engineering traditionally treats the relationship between the system and its operating environment. More pointedly, in the development of their argument for a "system of systems engineering" framework, Keating, *et al*. (2003) argue that as systems increase in complexity "it is naïve to think that problem definitions and requirements will be isolated from shifts and pressures stemming from highly dynamic and turbulent development and operational environments" (p. 38).

If it is naïve to think that complex systems are isolated from their operating environments, then how *should* system context be perceived in *Industrial Revolution 4.0*? For tomorrow's more complex systems, isolation should be traded for a more nuanced and comprehensive understanding of the operational environment surrounding system performance. In his support of the engineering systems approach described above, Long (2018) argued that "if we are to advance [systems engineering] in the right direction, we must advance, informed and guided by our *greater context*" (emphasis added). In response to technological developments, systems engineering should move beyond its long-held assumptions of clear boundaries and well-defined operating environments to derive system performance. Advanced systems engineering should move toward embracing variation, dynamism, and uncertainty in the system operational environment. This logic suggests that the "novelty" of the IR 4.0-based challenges to traditional systems engineering—increased autonomy, big data, and increasing complexity—may be related to how they change the relationship between systems, boundaries, and environments. For example, de Weck, *et al*. (2011) identify temporality as a key feature of complex systems. In so doing, system engineers are encouraged to examine what *may* change over the operational lifetime of the system—thereby explicitly addressing legacy issues, historical memories, and changes in assumptions about how the world works around systems.

Simply equating context with defining and meeting the business/technical needs of customers or as "well-known and controllable constraints" cannot account for variability in how humans will operate systems nor the potential impacts of changes in operational conditions, settings, or circumstances. For advanced systems engineering, this suggests that context is more than a set of variables to be held as constant or unidirectional, exogenous forces on interacting component behaviour. If, according to

*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. **SAND-PEER REVIEW.**

INCOSE Fellows (International Council on Systems Engineering (a), Undated), the added value of systems stems from the interconnectedness of their *component parts*, perhaps the value of advanced systems will stem from the interconnectedness of their *component parts* and *their operating conditions, settings,* and *circumstances*. Context for systems engineering would then evolve from an assumed static set of variables in closed systems and exogenous forces on component interactions in open systems to design and implementation variables interacting with components in advanced systems. These arguments echo claims that "systems engineering problems are evolving in ways suggesting contextual aspects of a complex system problem must be moved to the foreground" (Keating, *et al*., 2003, p. 38), to include better addressing the conditions, settings, or circumstances in which advanced systems will be operated.

3.4 Non-Traditional Approaches to Context in Advanced Systems Engineering

In response to technological evolution(s), advanced systems engineering should seek to more clearly and comprehensively describe operating environments—to include accounting for contextual descriptions consisting of the interrelated human behaviour, social, and organizational factors that impact system performance and success. Recent research in safety (Leveson N. G., 2012) (Stringfellow, 2010) and security (Anderson, 2008) (Williams, 2018) for complex systems illustrates the importance of including contextual influences in system design, operation, and evaluation. Yet, there is still a need to improve the ability of systems engineering to account for the role of context. Three academic literatures—systems theory, organization science, and engineering systems—offer insights to better understand and incoporate context into advanced systems engineering.

Systems-Theoretic Concepts and ***Insights***

Returning to core systems-theoretic concepts—and exploring their modern applications—lays a foundation upon which more comprehensively incorporate context into advanced systems engineering. Expanding on the Aristotelian argument that "the whole is more than the sum of its parts," general systems theory describes how observed behaviour(s) are not always explained by the behaviour(s) of the related component parts. In an attempt to address *organized complexity*—defined by Weaver (1948) as "problems which involve dealing simultaneously with a sizable number of factors which are interrelated into an organic whole"—systems theory provides a non-statistical, non-random logic to describe the behaviors of "many, but not infinitely many" (Von Bertalanffy, 1972, p. 415) components. From this perspective, a system constitutes a hierarchical order of processes in dynamic equilibrium driven by initial conditions, boundary constraints and external disturbances (Von Bertalanffy, 1950). These concepts have been observed in both the laws of physics (Von Bertalanffy, 1972) and sociology (Rasmussen, 1979). Additional observations across these disciplines indicate that systems naturally migrate toward states of greater disorder unless there are counteracting forces to maintain desired system behaviors. Observed advanced systems performance, then, can be described as system states resulting from initial conditions, boundary constraints, and external disturbances interacting with natural tendencies toward states of higher risk. This suggests two postulates for advanced systems performance. First, the same end state—or desired system performance—can be achieved with different internal dynamics (e.g., technological systems design) and initiating conditions (e.g., conditions, settings, and circumstances surrounding system use). Second (and similar to the results of the comparative study of CT scanners in hospitals by Barley, 1986), *different* end states can result from the *same* initiating conditions and internal dynamics.

Hierarchy and ***Emergence***

*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. **SAND-PEER REVIEW.***

A new take on two concepts from general systems theory—hierarchy and emergence—is instructive on how to account better for context in advanced systems engineering. Hierarchy refers to understanding the fundamental differences (and relationships) between levels of complexity within a system, including identifying what generates, separates, and links each level (Von Bertalanffy, 1950). Therefore, identifying what generates, separates, and links hierarchical levels is a vital aspect of system engineering to ensure that desired performance is achieved. A better understanding of the conditions, settings, and circumstances in which systems operate can more comprehensively describe the dynamics between hierarchical levels. Consider how new emissions regulations could change what separates and links how electric vehicles interact within the transportation system, for example.

Emergence refers to the phenomenon by which behaviors at a given level of complexity are irreducible to (and thus, cannot be explained by) the behavior or design of its subordinate component parts. Part of this irreducibility of observed system-level behaviors is driven by the system's interaction with the conditions, settings, and circumstances in which it operates. Consider how the impact of the internet as an information transfer system on current social practices cannot be explained by the protocols for transmitting digital packets of data, for example.

Hierarchy and emergence offer well known systems-theoretic concepts on which to build a better understanding of context in advanced system engineering. For both the electric car/transportation system and data packet/information transfer system examples, the context in which the designed systems are used serves an important role in achieving desired outcomes. Invoking these concepts relates advanced system performance to understanding how both component reliability and component interactions are influenced by the conditions, settings, and circumstances in which they operate.

The importance of contextual influences on advanced systems behaviour resonates with growing research related to system-theoretic causality models for emergent system properties. For example, recent work has leveraged the advances of Systems-Theoretic Accident Model and Process (STAMP) which argues that safety[1] of complex systems can be redefined as control over system behaviour that eliminates losses resulting from systems migrating into hazardous states and experiencing worst case environmental events (Leveson N. G., 2012). Related studies include system safety for the aviation (Fleming and Leveson, 2014), automotive (Placke, Thomas and Suo, 2015), medical (Pawlicki, *et al.*, 2016) and nuclear power ((Electric Power Research Institute, 2013) domains, as well as system security for cyber (Bakirtzis, Carter, Fleming, and Elks, 2017), transportation (Williams, 2015), and nuclear (Williams, 2013) applications. These studies argue that safety and security are not protecting against random failure problems but preventing the loss of control over desired system performance resulting from component interactions, dynamics, and (potentially) non-technical causes. Additional studies have also indicated that the system-theoretic causality model can capture human, social, and organizational influences—each representing elements of the conditions, settings, and circumstances of use—on system behaviors. Marais (2005) argues that these influences can be described as challenges to the effective implementation of controls over desired system behaviour(s). This study describes organizational risk factors as safety control flaws that violate design decisions intended to constrain unsafe system behavior. Building on this approach, Stringfellow (2010) demonstrated how incorporating human and organizational behavior-generated guidewords helped identify additional violations of STAMP-derived safety control actions—illustrating the role of context in complex systems performance.

[1] And, by extension, other similar *emergent* system properties such as security.

*Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525. **SAND-PEER REVIEW.**

The 2018 handbook for the Systems-Theoretic Process Analysis (STPA)—the analytical technique based on the STAMP causality model—expands this incorporation of contextual influences (Leveson and Thomas, 2018). According to the handbook, identifying particular loss scenarios that "describe the causal factors that can lead to the unsafe control actions and to hazards" (Leveson and Thomas, 2018, p. 42) is the last step for evaluating complex systems for safety. More specifically, this step can include changes to a controlled process itself, to the path for communicating control, or to how control is administered. This perspective of systems safety—which has shown improvements in safety of complex systems in the aforementioned domains—clearly articulates the importance of including the conditions, settings, and circumstances of use into advanced systems engineering. Applying these systems-theoretic concepts expands advanced systems engineering beyond technology-centric approaches and supports the role of contextual factors on system behaviors—particularly social, organizational, political, and cultural influences on human use of complex systems.

Organization Science Concepts and ***Insights***

If systems theory provides hierarchy and emergence of *technical* components to explain systems behaviors, then perhaps describing *non-technical* components in similar terms (or with similar concepts) can capture the importance of context in advanced systems engineering. Organization science, according to (Robbins, 1990), is an academic discipline[2] that studies the structure, behaviour, design, and internal dynamics of organizations—which can be loosely thought of as "human systems." Advanced systems engineering should explore how individuals construct institutions, processes and practices to achieve a common goal while implementing (or operating within) systems. For example, Argyris (1976) and Cyert and March (1963) 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 better explain the context in which advanced systems must operate.

Carroll (2006) argues that it is useful to investigate organizations from three distinct perspectives: the strategic design lens, cultural lens, and political lens. Each of these lenses represents shared ideas about human nature, the meaning of organizing, interpretation of collective goals, and the information required to make sense of an organization. Therefore, these three lenses also share descriptions of the context in which advanced systems operate. The *strategic design lens* argues that with the right plan, information flow, and resource distribution, the organization can be rationally optimized to achieve its goal. This lens aligns well with a traditional systems engineering understanding of context. The *cultural lens* describes organizational behavior in terms of the tacit knowledge of "this is how we do things around here" and the processes used to share this knowledge with newcomers. This lens emphasizes that systems are only understood in how they are actually used. Lastly, the political lens interprets organizations as diverse coalitions of stakeholders with different (and sometimes conflicting) interests whose performance is influenced by ever-changing power dynamics that influence decisions. This lens more explicitly identifies multi-dimensional

[2] "Organization science," "organization theory," and "organizational studies" are often used interchangeably to describe this academic domain. For example, the INFORMS journal *Organization Science*—a leading social science journal—explores organizational behavior and theory from strategic management, psychology, sociology, economic, political science, information systems, technology management, communications, cognitive sciences, and systems theory perspectives. For more, see: https://pubsonline.informs.org/journal/orsc.

*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. **SAND-PEER REVIEW.**

dynamics between components (or stakeholders) within a system and those in the environment. The *three lens* approach suggests that system performance assumptions underlying PPS designs are influenced by both the independent focal areas of and the interactions between each lens.

Two primary philosophical perspectives undergird the organization science analytical domain. The first is the *functionalist* perspective, which is an overall approach that seeks to rationally explain organizational phenomena based on observed relationships that can be identified, studied, and measured in similar manner to natural science (Burrell and Morgan, 1979). This perspective of technological systems reduces the introduction of technology into an organization as an exogenous force that changes the behavior of the organization itself or its attendant employees. In other words, the system and operating environment have a distinct boundary and there is a uni-directional causality from the system to its performance in its operating environment—much like traditional systems engineering approaches to context. Other characteristics of the functionalist perspective include an expectation of design dominance in performance, deterministic view of system operations, and designs based on the assumption that change in organizational behaviour is driven by technology (or, technological systems). Yet, only assuming that technological changes drive change within organizations dismisses the idea that these observed organizational changes might actually result in changes to the technological system itself.

The second primary perspective within organization science is the *constructivist* approach, which seeks to explain organizational phenomena in terms of individual perspectives and in terms of processes that emerge from the resultant interpretive flexibility between these individual perspectives (Burrell and Morgan, 1979). From this perspective, humans are seen as creating technological systems under the influence of a set of socially constructed norms, assumptions and beliefs. Once implemented, the effect of these technological systems on organizations is understood as a set of (not necessarily the same) socially constructed norms, assumptions, and beliefs. Here, systems and operating environments have similarly distinct boundaries, but the uni-directional influence is from the external operating environment to the system—a perspective diametrically opposed to a functionalist approach. Other characteristics of this perspective include an expectation of system design stabilization, interpretive flexibility of system operations over time, and assumptions that organizational change is drive by socially (re)structured relationships between human users and technological systems. Where the constructivist perspective does consider the (often-assumed as unnecessary or extraneous) social context surrounding technological systems as vital, there does not seem to be much room for these emergent social constructs to be influenced by the technological system itself.

Between these two primary philosophical perspectives of organization science lies a theory that argues organizational behaviors are not *either* driven by technological systems *or* interpreted by users of technological systems, but rather are a result of both. Structuration theory asserts that organizational behavior emerges from recurrent human action that is both (and simultaneously) shaped by technological artifacts and constructed by their interpretation (Giddens, 1984). In this perspective, there is more ambiguity in and interactions between systems and their operating environments. The origins of Giddens' (1984) structuration theory (or, the enactment of structure) expanded into a spectrum of descriptions of the recursive interactions between humans, technology, and organizations. Where functionalist approaches argue that change is driven by technological systems and constructivist approaches argues that change is driven by interpretation of technological systems in use, structurational approaches assert that change is driven by recursive and recurrent use

*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. **SAND-PEER REVIEW.**

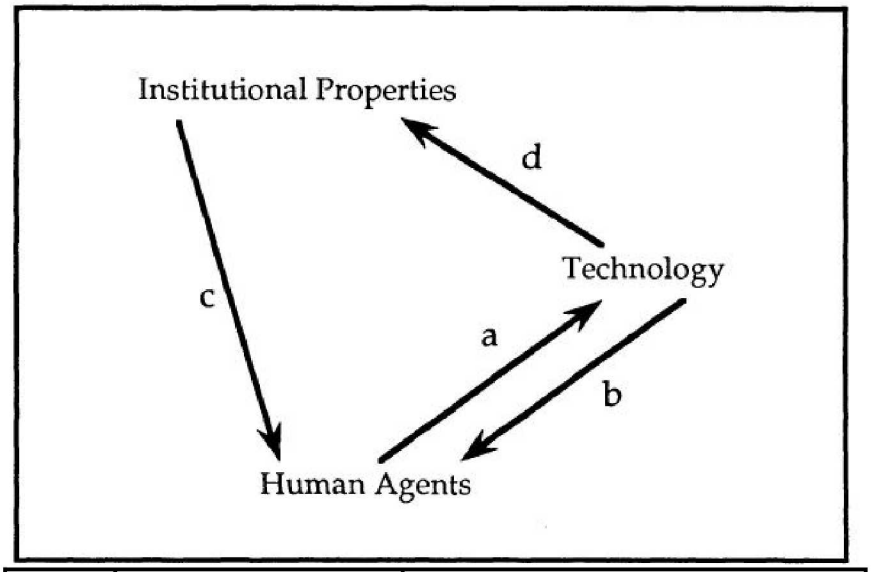
of technological systems. Other characteristics of this perspective include an expectation of recurrent use of designs, dynamic understanding of a system's operating environment, and an assumption that change results from regular patterns of system use and observed performance. Structuration theory offers a perspective that accounts for both the effects of the technological system on its operating context and the effects of its operating context on the technological system itself.

Structuration theory further asserts that organizational structure is a dynamic process seeking equilibrium via recurrent human actions. This assertion is typified by Giddens' (1984) argument that, despite the circumstances or context, an individual always has an option to change their response to the current organizational structure. This perspective also argues that structure always both enables and constrains performance and outcomes. Organizational structure, then, either reinforces or transforms desired performance, suggesting that both continuity and change require a balance between supporting current designs and adapting to changes in the operating environment. By replacing "organization" with "system" and "individual" with "component," structuration theory provides a useful logic incorporating context into advanced systems engineering.

The interactions between technology and organizations in structuration theory align well with the general systems theory phenomenon where interdependence among components is influenced by, and influences, the operating environment. For example, in a study on implementing self-served internet technologies in the health insurance domain, Schultze and Orlikowski (2004) show "how macrophenomena are constituted by microinteractions, and how these microinteractions, in turn, are shaped by macro influences and effects (88)." Structuration and systems theories share additional conceptual commonalities. Consider the similarities between the *enactment* (e.g., resulting from recurrent human use) of technological systems in the former with *emergence* of systems behaviour (e.g., from regularly interacting components) in the latter. They also share a lexicon, including dynamism, complexity, equilibrium, and interdependence. Both theories also assert that a focus on transitioning between *steady* state A and *steady* state B—as opposed to *stable* state A and *stable* state B—better addresses the complexity present when social and technological components interact.

Orlikowski's (1992) Structurational Model of Technology (SMOT) serves as an instructive example of the importance of context in explaining emergent behaviors. SMOT describes recursivity in how *human agent* actions situate the use(s) of *technology*, which then shapes the enacted organizational structure that produces *institutional properties* that enable or constrain those *human agent* actions (Figure 1). By replacing *technology* with *system*, the traditional systems engineering perspective gives way to a perception of system performance as resulting from the interaction(s) of technological components as used by human agents under the influence of institutional properties. For example, from the SMOT perspective, performance of vehicle manufacturing systems is not a singular product of production rates, but rather a descriptor of the capability of human agents to use the system (under the influence of institutional properties) to produce the appropriate number of cars to meet societal need and regulatory requirements. The technologies that compose a complex system also shape the enacted structure of the organization and the resulting institutional properties influencing its performance. For example, nuclear power plants that rely on advanced digital controllers for safety critical sub-systems have different enacted structures than those that rely on more traditional analog controllers. According to SMOT, institutional properties can either reinforce or oppose desired human use of technology—further supporting the important role that use context plays in ensuring complex systems achieve their designed objectives.

*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. **SAND-PEER REVIEW.**



ARROW	TYPE OF INFLUENCE	NATURE OF INFLUENCE
A	Technology as a Product of Human Action	Technology is an outcome of such human action as design, development, appropriation, and modification
B	Technology as a Medium of Human Action	Technology facilitates and constrains human action through the provision of interpretive schemes, facilities, and norms
C	Institutional Conditions of Interaction with Technology	Institutional Properties influence humans in their interaction with technology, for example, intentions, professional norms, state of the art in materials and knowledge, design standards, and available resources (time, money, skills)
D	Institutional Consequences of Interaction with Technology	Interaction with technology influences the institutional properties of an organization, through reinforcing or transforming structures of signification, domination, and legitimation

Figure 1. Orlikowski's Structurational Model of Technology (SMOT) (Orlikowski, 1992).

The logic of SMOT offers two useful insights for describing the relationship between systems and the conditions, settings, and circumstances in which they operate. First is the direct and recursive relationship between human agents and technology (or, technological systems). More explicitly understanding these dynamics are necessary as systems continue to advance and grow in complexity to meet increasingly difficult—and constantly changing—social needs. For example, the internet as a mass communication and information sharing system looks markedly different today than its designers intended "because if we had known what it would turn into, we would have designed it differently."[3] The second insight is the role of institutional properties in directly influencing human and being directly influenced by the technology (or, technological system) itself. Thus, advanced systems engineering needs to address sources of institutional properties—which can range from cultural norms to societal needs to regulatory requirements to organizational policies. Additionally, advanced systems engineering has the potential to transforms these institutional properties. For this second insight, the internet as a complex system is again instructive when considering current debates on net neutrality, cryptocurrencies, and exploitation of the "deep web" for malicious

[3] This quote is from Dr. David Clark, chief protocol architect in the development of the, during his lecture to the Fall 2012 offering of *Engineering Systems Doctoral Seminar* (ESD.83) at the Massachusetts Institute of Technology. For more about the designing of the internet, see Clark, 2018.

*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. **SAND-PEER REVIEW.**

purposes. As such, structuration theory helps crystallize some key insights from organization science that support the case for—and provide mechanisms to incorporate—the importance of context in advanced systems engineering.

Engineering Systems Concepts and ***Insights***

Yet, there is still a need to more formally integrate these organizational science insights into advanced systems engineering. Engineering systems[4] is a growing academic discipline that seeks to develop theory and practice related to characterizing and analyzing the complex causality describing large, technical system behaviors in their social and political contexts. With this perspective and several key characteristics established in de Weck, *et al.* (2011), engineering systems offer a way to reconcile these insights to explain advanced system performance as "characterized by a high degree of technical complexity, social intricacy, and elaborate processes, aimed at fulfilling important functions in society" (de Weck, Roos, and Magee, 2011, p. 31). More specifically, Table 1 summarizes the definitions of the primary characteristics that distinguish an engineering systems perspective from traditional system engineering approaches.

Table 1. Definitions of Key Characteristics of the Engineering Systems

	Definition from de Weck, *et al.* (2011)
Function	"action for which a thing is specifically fitted or used, or the reason for which a thing exists" [p. 51]
Scale	"geography, demography, numbers of components, number of people, and any other aspect that can be used to assess the size of the system *quantitatively* (emphasis in original)" [p. 50]
Scope	"the number of aspects that need to be considered when defining the system" [p. 50]
Structure	"the way in which elements of the system are interconnected…also includes assignments of sub-functions to the elements of the system'"[52]
Temporality	"dynamic; [the systems] change with time…[the] time scale[s] that agents, mass, energy, and information flow through complex engineering systems" [p. 55]

In an essay supporting this perspective of systems engineering evolution, (Long, 2018) noted the importance of correctly understanding the operational context when he underscored "a team of *systems engineers working in concert with the right subject matter experts* to understand the problem and characterize the solution can be a thing of beauty delivering elegant solutions to complex problems" [emphasis added]. This discipline's incorporation of technology, management and social science highlights the importance of context, or the confluence of dynamic, exogenous factors that influence how system behaviors propagate, shape how stakeholders interact, and bound how systems operate. For example, an engineering systems approach explicitly includes the impact of changes over time and different timescales of these changes on system design, implementation, and evaluation. Consider U.S. nuclear power plants built 60+ years ago that are undergoing operating life extension license renewals, are replacing analog components with digital controllers, and are simultaneously faced with competing against historically low natural gas prices. This characteristic of engineering systems highlights the interactive role of context on advanced system performance.

[4]This academic discipline was pioneered by the *Engineering Systems Division* (ESD) at the Massachusetts Institute of Technology, which aimed to focus on the science and engineering of large and complex socio-technical systems by leveraging insights across academic disciplines. In 2015, ESD subsumed by the *Institute on Data, Systems,* and *Society*—for a thoughtful obituary of this program, see de Weck O. , 2016.

*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. **SAND-PEER REVIEW.**

Reframing the characteristics of engineering systems provides organizing principles by which to reconcile the different aspects of systems theory and organization science to develop a better understanding of the *context of use* for advanced systems.

3.5 *Context of Use* in Advanced Systems Engineering

If human (inter)actions can influence the structure, boundaries, and dynamics of how systems operate, then systems engineering needs new mechanisms for addressing this new understanding of context. Leveraging insights from the systems theory, organization science, and engineering systems disciplines can help develop how to better account for context in advanced systems engineering. Context of use is important because, as argued by Bucciarelli (2003), with advanced systems "...different participants, with different technical responsibilities and interests, see the object of design differently" (p. 13). Further, from his philosophy of science perspective, Bucciarelli (2010) also introduces two different fundamental descriptors of a designed object—either "value-free" or "context of use." Though Bucciarelli was writing about technological widgets in general, replacing "designed object" with "advanced system" is helpful. From a "value-free" engineering design standpoint, focusing on the "formal structure" removes such sticking points as social, political and cultural issues and aids in more expedient system implementation. This perspective seems to support the logic that a well-designed operating system can operate independently of contextual influences and thus can be an element of common ground among multiple stakeholders. Or, as Bucciarelli (2010) puts it "There is the mutual trust in abstraction itself" (p. 21).

Conversely, Bucciarelli (2010) asserts that "context of use"-based design can translate into better solutions. This perspective seeks to more explicitly include social, political, and cultural influences on system design and implementation, allowing systems-theoretic trade-offs to be better manipulated to address the problem at hand. This perspective can also allow an already existing technology (or system) to be more effective. Consider how well Apple products sell, even though oftentimes the technology on which they are based has been around for years (e.g., the touch screen). Ultimately, the use of "formal structures" can help shape and improve design discussions within systems engineering, but "context, the circumstances and conditions within which a complex systems problem is embedded, can constrain and overshadow technical analysis determining system solution success" (Keating, *et al.*, 2003, p. 38). As such, the *context of use* for advanced systems engineering can be described as the conditions, settings, and circumstances in which a system operates, including the dynamic, interdependent factors of a system's embedded environment that bound how it operates, influence how its behaviors propagate, and shape how its stakeholders interact.

To do so requires more than shifting from a closed to an open systems perspective. In the former, a system's environment is simply a universal constraint with an immutable boundary. In the latter, context is not completely discounted, as a system's environment is considered sets of bounding conditions or guidelines to satisfy exogenous forces on desired system behaviors. Yet, neither of these perspectives capture how "contextual, human, organization, policy, and political system dimensions that will ultimately shape the decision space and feasible solutions for the technical system problems" (Keating, *et al.*, 2003, p. 39). Discounting these influences reduces design and development to predetermined "correct" uses of advanced systems—drastically limiting their success to an artificially narrow sliver of the problem space. Therefore, the context of use for advanced systems engineering leverages insights from strucration theory to move toward capturing how "everyday actions are consequential in producing the structural contours of everyday life" (Feldman

*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. **SAND-PEER REVIEW.**

and Orlikowski, 2011, p. 1241). As such, the conditions, settings, and circumstances in which systems operate are more than constraints affecting advanced systems, they are now important variables impacting system performance.

The context of use perspective addresses how the impact of systems engineering (including the associated problem and potential solution spaces) is always larger than the associated technological basis of the system itself. For instance, this context of use perspective can help explain the engineering systems paradigm from MIT where advanced systems are "socially transformative" (de Weck, Roos, and Magee, 2011). Similarly, the engineering systems emphasis on better understanding of emergent system properties—the so-called "ilities"[5]—seemed to (at least partially) emerge directly from this larger context of use concept in systems engineering. The role of context of use is also seen in how a system's network structure can be designed to propagate diffusion of desired behaviors, how contextualized understanding of socio-technical systems influences stakeholder interactions, and how context of use is a driving force for technological changes over time. Context of use is also captured in assertions made by Keating, *et al.*, (2003) that "metasystems are themselves comprised of multiple autonomous embedded complex systems that can be diverse in technology, context, operation, geography, and conceptual frame" (p. 41). Therefore, for systems-of-systems to achieve their objectives, they argue, metasystems act as the conditions, settings, and circumstances for the embedded systems—not a static or unidirectional operating environment, but an interactive and interdependent context of use.

Better understanding a system's context of use can also help alleviate the increase in system performance uncertainty stemming from increases in system complexity. Where emergence is a vital characteristic, more systems complexity expands possibilities for unanticipated outcomes that can be missed by traditional systems engineering approaches. Rather than allowing uncertainty to limit system success, advanced systems engineering should track changes in the context of use to anticipate any "unexpected" shifts in system performance. For big data, this idea argues that it is not the quantity of information available that helps mitigate increasing system complexity, but the capacity to use that information in meaningful ways to achieve desired system performance within the conditions, settings, and circumstances in which it operates.

3.6 Example: Systems-Theoretic Framework for Security

To further make the case for including the context of use in advanced systems engineering, this section will explore improving systems engineering approaches for security at high consequence facilities. Here, the objective of security is to protect the high consequence (or high value) facility from malicious or intentional acts that could result in such unacceptable losses as human fatality or injury, theft or loss of assets, damage to property/infrastructure, or environmental destruction or contamination (e.g., nuclear or chemical facilities). Security at high consequence facilities—be they chemical plants, oil refineries, nuclear power plants, or other pieces of critical infrastructure—is typically provided by a combination of sensors, cameras, barriers, and other technologies called a *physical protection system* (PPS) with the objective to detect, delay, and respond to malicious acts.

---

[5] Per de Weck, *et al.* (2011), the *ilities* are "are desired properties of systems…[that] are not primary functional requirements of a system's performance, but typically concern wider systems impacts with respect to time and stakeholders than are embedded in those functional requirements" (p. 66). Examples include flexibility, reliability, and adaptability.

*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. **SAND-PEER REVIEW.**

Adequately selecting, arranging, installing, operating, and maintaining these interconnected PPS components are major challenges to ensuring security of high consequence facilities. To demonstrate the value of the context of use in advanced systems engineering, two approaches for resolving these challenges to security will be compared. The first approach is based on traditional systems engineering approaches, whereas the second approach incorporates the context of use to expand the solution space for security at high consequence facilities.

A Traditional Systems Engineering Approach: Design Evaluation Process Outline (DEPO)

Building on generic systems engineering concepts such as feedback processes and hierarchical design, high consequence security becomes the process of appropriately determining, designing and evaluating PPS. One of the most popular—and most prolific—high consequence security methodologies is the Design Evaluation Process Outline (DEPO) developed at Sandia National Laboratories. More specifically, DEPO is the current standard for security analysis at nuclear facilities around the world. The DEPO methodology is popular for its clarity and stochastic modeling paradigm that concludes when balance is achieved between the level of risk and upgrade impact to facility budget and operations concerns (Garcia, 2008). The traditional systems engineering basis of DEPO also borrows a philosophical foundation from applying probabilistic risk assessment (PRA) {REF} to nuclear safety. The accident timeline is replaced by the competing timelines of required adversary action to achieve a malicious act and the response force actions necessary to protect the high consequence facility. The DEPO methodology describes security as probabilistic influences on this timeline—the probability that a particular sensor alarms when an adversary enters a prohibited area or the probability that the response force is able to intercept the adversary, for example.

As illustrated in Figure 2, DEPO consists of three primary functions: determining the PPS objectives, designing the PPS, and evaluating the PPS (Garcia, 2008). Determining PPS objectives consists of four aspects: *characterizing the facility* (e.g., What is its mission? Where is it located? Who works at it?); *identifying undesired events* and *critical assets* (e.g., what are the potential targets); *determining consequences of undesired events* (e.g., what is the facility liability or regulatory responsibilities); and, *defining threats to the facility* (e.g., what are the capabilities of the adversary according to national threat assessments and local factors). Once the objectives are defined, the DEPO methodology is used to design the PPS itself. Here, the PPS design is analyzed for system effectiveness using different heuristics to identify, down-select, arrange and optimize the characteristics of security-related technologies to achieve delay, detection, and response goals. Lastly, DEPO requires an evaluation of the PPS, which includes *estimating the risk* (as related to system effectiveness against malicious acts) and *comparing this risk to the acceptable risk levels*. Consistent with traditional systems engineering concepts, if the risk is sufficient, the (re)design is complete; if it is insufficient, modifications (or upgrades) to the PPS should be suggested and reevaluated. By this process DEPO uses the "detect, delay, and respond" paradigm to fully describe –and engineer PPS to meet—the necessary functions of strong security for high consequence facilities (Garcia, 2008).

DEPO calculates the ability of an arranged collection of technologies to defeat a specific adversary along a specific attack path. This methodology relies on two probabilistic descriptors of security performance. The first is the *probability of interruption* (P_I), or the conditional probability that detection and delay system components will *assess* an adversary in time for response forces to arrive onsite to engage. The second is the *probability of neutralization* (P_N), or the conditional probability that, upon arriving, response force capabilities can kill, capture or cause the adversary to flee. P_I and

*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. **SAND-PEER REVIEW.**

P_N are nested, conditional probabilities related to security system component performance derived from performance testing (at best) or (at worst) expert opinion. DEPO defines the ability to adequately protect high consequence facilities as the *system effectiveness (P_E)* of the PPS—itself the product of P_I and P_N. More specifically, DEPO employs the risk formula $R = P_A*(1-P_E)*C$. Here, P_A is the assumed probability of attack; C is a quantitative approximation of qualitative consequence descriptions; and P_E is the system effectiveness. Given the difficulty in of accurately quantifying P_A, DEPO best practice is to use a "conditional risk" (where $P_A = 1$) that simplifies the equation to $R_C = (1-P_E)*C$.

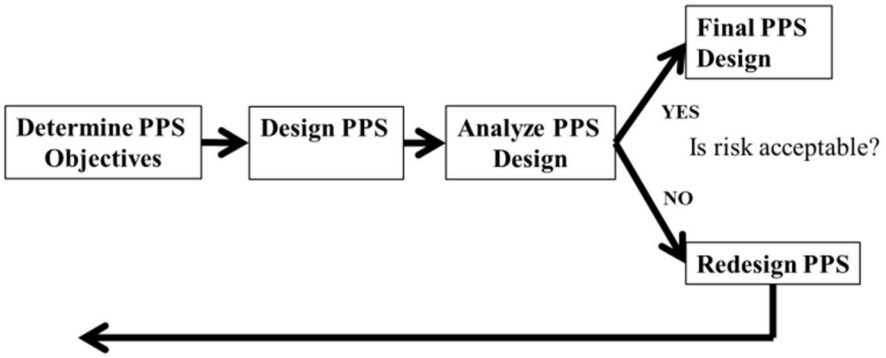


Figure 2. Illustration of DEPO Methodology Recreated from Figure 1-1 (Garcia, 2008).

The traditional focus on technological system solutions in DEPO is based on the implicit assumption that any PPS can achieve desired levels of performance regardless of the operational context. This is an oversimplified and untenable assumption at the core of DEPO-based approaches that negates the impacts of contextual influences on security performance at high consequence facilities. Consider, for example, a visit by Dr. Matthew Bunn[6] to a Russian nuclear institute in the mid-2000s where he recounted that:

> …inside the hallway leading to the vault where a substantial amount of weapons-grade nuclear material was stored, there were two portal monitors that personnel had to pass through, one after the other, an American machine and a Russian machine. When asked why, the site official conducting the tour said that the building next door made medical isotopes, and on Thursdays, when the chemical separations were done to get the desired isotopes from the remainder, so much radiation went up the stack that it set off the American-made portal monitor. So on Thursdays, they turned off the American-made monitor and relied on the less sensitive Russian one. Of course, every insider was aware of this practice, and would know to plan an attempted theft for a Thursday, making the existence of the American portal monitor largely pointless. (Bunn and Sagan, 2014, p. 11)

[6] Former nuclear security advisor to the Office of Science and Technology Policy; current Professor of Practice at Harvard University's Kennedy School of Government and co-Principal Investigator for the Project on Managing the Atom.

*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. **SAND-PEER REVIEW.**

Relying on traditional systems engineering-based approaches—like DEPO—would indicate the same estimate for PPS effectiveness even *after* this observation of its use. In other words, there is still a need to better understand the relationship between the technical system (e.g., American portal monitors of the PPS to detect unexpected radioactivity), the technical system's context of use (e.g., turning off the American portal monitors to avoid high levels of false alarms from medical isotope production on Thursdays), and security performance (e.g., reduced detection capability and increased opportunity for a malicious act by an adversary).

Systems-Theoretic Framework for Security (STFS)

Based on the previous anecdote, part of a security system's context incudes the capability of the security organization oversee the correct use of the PPS in pursuit of strong security performance. In response, the Systems-Theoretic Framework for Security (STFS) argues the need to include *some* measure of *context* in security for high consequence facilities. Using a non-traditional perspective to build on traditional systems engineering concepts, STFS provides an approach to better explain security performance. First, consider that actual security performance is impacted by individual actions during daily security work practices, the PPS, and the security organization—and their interactions. Second, the current level of performance influences both the PPS itself and the security organization (e.g., feedback). Here, if daily work practices help explain these feedback and interaction dynamics, then security performance emerges from how individual security actions are influenced by the technology within the PPS itself and the organizational factors that affect its use context. The technological availability relates to how well the PPS meets its detection, delay, and response objectives *within* a given operational context. The organizational factors relate to aspects of the conditions, settings, and circumstances in which the PPS operates that affects daily work practices. Security performance, then, results directly from how well the PPS design operates (e.g., how it meets the P_E objectives) and indirectly from how the security organization affects individual security actions.

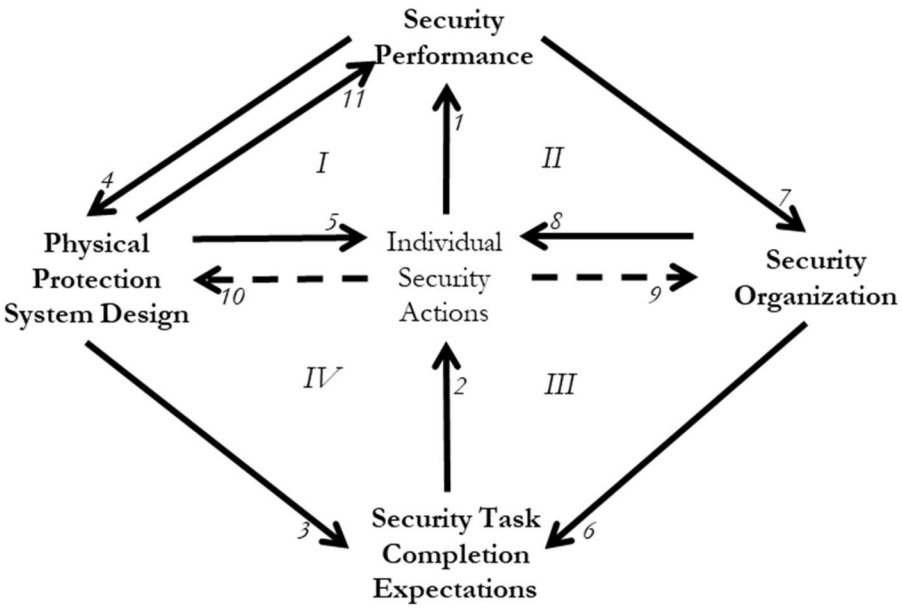


Figure **3** . Overview of the Systems-Theoretic Framework for Security

Solid arrows [⟶] indicate currently recognized influences and dashed arrows [- - -⟶] indicate influences unrecognized by current state-of-the-art approaches.

*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. **SAND-PEER REVIEW.**

As illustrated in Figure 3, STFS describes security performance in terms of five *elements* (e.g., denoted with bold text), eleven *links* (denoted with numbered arrows), and four *feedback loops* (denoted with Roman numerals). These elements represent both tangible and intangible attributes that interact and result in security performance. More specifically, these elements are *security performance* (completion and quality of detection, delay, and response functions); *individual security actions* (work practices that support achieving PPS security functions); *security task completion expectations* (contextual conditions for work practices to support the PPS); *security organization* (entity taking actions and making decisions to operationalize the PPS); and the *physical protection system design* itself. The STFS elements are connected by *links* that describe causality and functional roles within the framework. The causality of each link is expressed in terms of how the sending STFS element interacts with the receiving STFS element. For example, the monitoring and evaluation role of Link 4 should be read as "Security performance *provides* assessment of technical performance as observed by inspection results, corrective actions or response to a security event *to* the security organization." These links, summarized in Table 2, partially describe the conditions, settings, and circumstances in which PPS operates—explicitly incorporating the *context of use* into an advanced systems engineering approach to security at high consequence facilities.

Table 2. Summary of link descriptions for the Systems-Theoretic Framework for Security.

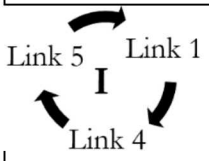
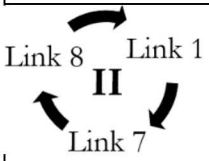
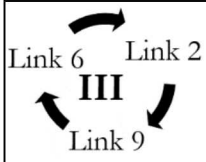
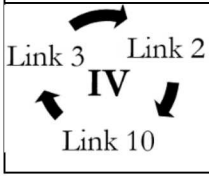
#	Name	Description
1	Security task completion	Which (e.g., actual P_E) and how well (e.g., quality indicators) security functions are achieved
2	Influence of Expectations	CONOPs, procedures and behavioral performance requirements defining necessary security tasks
3	PPS-based requirements	Necessary actions expected by designers to achieve estimated system effectiveness ($\sim P_E$) for a particular PPS design
4	Feedback on technical performance	Assessment of technical performance as observed by inspection results, corrective actions or response to a security event
5	Technical availability for security	Security-related technologies implemented to achieve expected security functions* (e.g., $\sim P_E$)
6	Organizational expectations	Decisions on the necessary and sufficient actions (e.g., resources provided) to support the expected PPS performance
7	Feedback on organizational performance	Assessment of organizational performance as observed by inspection results, corrective actions or response to a security event
8	Behavioral quality for security	Operational context in place to achieve expected security functions (e.g., data-derived organizational influences)
9	Human behavior effects (Quality)	Recurrent security-related actions of individuals that describe how the PPS is used (e.g., patterns of security practice)
10	Human behavior effects (Structure)	Recurrent security-related actions of individuals that describe what in the PPS is used (e.g., patterns of security practice)
11	Actual PPS Capacity	Capability and reliability with which technical components achieve expected security functions (e.g., traditional DEPO)

The links describing causality also represent the dynamic, interactive relationships between elements that identify interdependency between the PPS (as a technical system) and its context of use. Connected sets of links form *feedback loops*—relationships wherein output of a system (or process)

*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. **SAND-PEER REVIEW.**

returns as new input into the same system (or process). These feedback loops help describe the complex, nonlinear behaviors observed in nuclear security performance. In addition, interacting feedback loops provide an opportunity to describe more complex nuclear security performance behaviors, including the effect of the contextual influences on security performance described in the Bunn account above. These four feedback loops (summarized in Table 3) capture the dynamics often assumed with security design for high consequence facilities (Loop I), offer deeper explanations of contextual influences (Loops II and III), and illustrate the interactions between systems and their operational environments (Loop IV).

Table 3. Summary descriptions of feedback loops for the Systems-Theoretic Framework for Security.

Feedback Loop	Summary Description
	Technical feedback based on formal monitoring and oversight (capturing traditional DEPO-based approaches and dynamics)
	Organizational feedback based on formal monitoring and oversight (capturing traditional security culture model-based dynamics)
	Observational feedback based on patterns of security behavior (capturing the dynamics between organizational decisions, security task completion and individual security actions)
	Observational feedback based on patterns of PPS use (capturing dynamics between the PPS, security task completion and individual security actions)

The STFS uses *elements* (key attributes), *links* (descriptions of causality) and *feedback loops* (dynamic relationships) to build on traditional systems engineering approaches (e.g., DEPO) to include the role of the context of use in security for high consequence facilities. In addition, the STFS provides the ability to ask why actions were taken or decisions made in the operational environment and trace their ramifications to PPS performance, which can illuminate additional causal factors affecting security performance. By doing so, the STFS provides a mechanism for describing how the interactions between technical systems and use contexts can better describe emergent properties in advanced systems. By including the context of use, the STFS offers several new insights for understanding nuclear security performance. First, this framework articulates that security performance is a system-level property based on both the technical ability of the PPS and how it is operated (e.g., behavioral quality). The STFS captures the dynamics of traditional DEPO-based

*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. **SAND-PEER REVIEW.**

approaches (that emphasize PPS ability) in Feedback Loop I, but also helps explain how different interactions between technical ability and behavioral quality result in a range of security performance outcomes.

This context of use is not intended to describe operational reality *perfectly*, but rather to serve as a signal directing attention toward possible security vulnerabilities and PPS performance inadequacies not included in traditional DEPO system effectiveness calculations. For some PPS components, the potential for contextual factors to challenge acceptable performance and change observed behaviors will be limited—the ability of 0.5 meter thick wall of an underground storage vault to provide delay, for example. For others, though, contextual factors present greater opportunities to challenge acceptable performance and change observed behaviors—turning off the portal monitors in the Bunn anecdote degraded the ability to meet detection objectives, for example. Similarly, where DEPO-based approaches are based on the analytic assumption that security personnel will use the PPS as expected by designers, the STFS captures how the context of PPS use may deviate from expectation.

In maintaining the role of technical PPS in security performance, an advanced systems engineering approach (e.g., the STFS) extends traditional systems engineering approaches (e.g., DEPO) to analysis of security at high consequence facilities to better account for the dynamics interactions with their context of use and the resultant effects on traditional performance metrics (e.g., P_D, t_D and RFT). Though not attempting to explain all aspects of security at high consequence facilities, the STFS provides an advanced systems engineering framework that captures the use context of security in terms of simple feedback loops and observable patterns of system behavior. The implication that security performance is not a static attribute of such facilities indicates a need to shift from optimizing PPS designs toward equilibrating between technical systems and operational contexts toward desired levels of performance.

3.7 Summary

Summarizing the context of use, the effects of system engineering solutions are wider ranging than their intended technological problem space. Systems can be better designed, better implemented, and more effective when accounting for the conditions, settings, and circumstances in which systems operate. As the challenges and changes of the *Industrial Revolution 4.0* manifest, the relationship between "system" and "operating environment" will be increasingly important—especially as social, political, and cultural influences continue to evolve. The difference between the STFS and DEPO-based approaches to security at high consequence facilities demonstrates how the ability of a PPS to adequately achieve desired levels of performance can be affected—both positively and negatively—by dynamic interactions with its context of use. This is illustrative of how advanced systems engineering can incorporate the context of use to improve system performance. Advanced systems engineering should explore the commonalities between key concepts in systems theory, organization science, and engineering systems to develop additional analytical capabilities to address the role of context and improve the increasingly complex systems of the future.

In this regard, Keating, *et al*., (2003) offer four questions around which to craft new analytical techniques for including the context of use into advanced systems engineering:

(1) What are the relevant contextual aspects of the system-of-systems engineering effort?
(2) Has the engineering process accounted for the contextual nature of the effort?

*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. **SAND-PEER REVIEW.**

(3) Has an appropriate balance been struck between the technical and contextual aspects of the problem?
(4) Can this balance shift over the system-of-systems engineering effort?

Providing the basis for advanced systems engineering capabilities to address these questions is the foundation of the context of use concept—and the benefits of doing so were demonstrated in the comparison of traditional and advanced systems engineering approaches to security at high consequence facilities. Describing security as a result of patterns of practice and feedback loop dynamics aids in identifying potential interventions for improving performance. For example, advanced system engineering approaches could seek to redirect oppositional contextual influences—and undesirable socio-technical interactions—to support desired system-level behaviors. By invoking systems theory, organization science, and an engineering systems approach, the context of use helps to redefine desired complex system properties in terms of aligning interacting technical systems and the conditions, settings, and circumstances in which they operate.

Moving forward, advanced systems engineering will likely need to more explicitly incorporate patterns of use into system design. As described, the context of use offers to the ability to better ensure consistency in performance of the *same* complex system in *similar* operating environments with *different* contexts—overcoming the challenges experienced in Barley's (1986) analysis of why implementing the same set of CT scanners in similar hospitals had drastically different results or Williams' (2018) evaluation of different security performance outcomes from the same physical protection system being implemented a similar high consequence facilities. Similar to Leveson's (2012) argument that evaluting emergent system properties can help explain unexpected systems behaviors (especially in the absence of component failure), including the context of use offers an additional perspective by which to explain such unexpected system behaviors. To the extent that the context of use paradigm is beneficial, it also serves as a mechanism by which to incorporate new ideas and analytical frames from other disciplines. Here, two examples include advances in applying structuration theory to technology (DeSanctis and Poole, 1994) and the use of assumption-based planning concepts in developing leading indicators for complex system behaviors (Leveson N., 2015). Further, this context of use perspective offers a wider range of potential explanations for—and levers to correct—unexpected system behaviors and reducing opportunities for "unintended consequences." In short, the need to understand and incorporate the context of use in design and analysis of complex, socio-technical systems is one of the most unique characteristics facing advanced systems engineering.

References

Anderson, R. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems* (2 ed.). John Wiley and Sons.

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

Bakirtzis, G., Carter, B. T., Fleming, C. H., and Elks, C. R. (2017). MISSION AWARE: Evidence-Based, Mission-Centric Cybersecurity Analysis. *arXiv preprint arXiv:1712.01448*.

*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. **SAND-PEER REVIEW.**

Barley, S. R. (1986). Technology as an occasion for structuring: Evidence from observations of CT scanners and the social order of radiology departments. *Administrative Science Quarterly, 31*, 78-108.

Biringer, B., and Danneels, J. (2000). Risk Assessment Methodology for Protecting Our Critical Physical Infrastructures. *Risk-Based Decision Making in Water Resources IX.* Santa Barbara: ASCE.

Bucciarelli, L. L. (2003). Designing, Like Language, is a Social Process. *Engineering Philosophy*, 9-22.

Bucciarelli, L. L. (2010). *From Function to Structure in Engineering Design.* Cambridge, MA: Massachusetts Institute of Technololgy. Retrieved from https://dspace.mit.edu/handle/1721.1/51789

Bunn, M., and Sagan, S. (2014). *A worst Practices Guide to Insider Threats: Lessons from Past Mistakes.* Cambrdge, MA: American Academy of Arts and Sciences.

Burrell, G., and Morgan, G. (1979). *Sociological Paradigms* and *Organizational Analysis.* London: Heinemann.

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

Clark, D. (2018). *Desgining an Internet.* Cambridge, MA: MIT Press.

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

de Weck, O. (2016, March/April). MIT Engineering Systems Division R. I. P. Eulogy for a successful experiement 1998-2015. *MIT Faculty Newsletter, XXVIII(4)*. Massachusetts Institute of Technology. Retrieved from http://web.mit.edu/fnl/volume/284/deweck.html

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

DeSanctis, G., and Poole, M. S. (1994). Capturing the complexity in advanced technollogy use: Advanced structuration theory. *Organization Science, 5*(2), 121-147.

Electric Power Research Institute. (2013). *Hazard Analysis Mathods for Digital Instrumentation* and *Control Systems Technical Report 3002000509.* Electric Power Research Institute.

Feldman, W. S., and Orlikowski, W. J. (2011). Theorizing Practice and Practicing Theory. *orginization Science, 22*(5), 1240-1253.

Fleming, C. H., and Leveson, N. G. (2014). Improving Hazard Analysis and Certification of integrated Modular Avionics. *Journal of Aerospace Information Systems, 11*(6).

*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. **SAND-PEER REVIEW.**

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

Giddens, A. (1984). *The constitution of society: Outline of the theory of structuration.* University of California Press.

Glass, R. J., Beyeler, W. E., Ames, A. L., Brown, T. J., Maffitt, S. L., Brodsky, N., . . . Linebarger, J. M. (2012). *Complex Adaptive Systems of Systems (CASoS) Engineering* and *Foundations for Global Design (*SAND*2012-0675).* Albuquerque, NM: Sandia National Laboratories.

Hall, J. L. (2003). Columbia and Challenge: organizational failure at NASA. *Space Policy, 19*, 239-247.

International Council on Systems Engineering (a). (Undated). *A Consensus of INCOSE Fellows: Definition of a System*. Retrieved from INCOSE.org: https://www.incose.org/about-systems-engineering

International Council on Systems Engineering (b). (Undated). *What is Systems Engineering?* Retrieved from INCOSE.org: https://www.incose.org/about-systems-engineering

Keating, C., Rogers, R., Unal, R., Dryer, D., Sousa-Perez, A., Safford, R., . . . Rabadi, G. (2003). System of Systems Engineering. *Engineering Management Journal, 15*(3), 36-45.

Kenett, R. S., Zonnenshain, A., and Swarz, R. S. (2018). Systems Engineering, Data Analytics, and Systems Thinking: Moving Ahead to New and More Complex Challenges. *INCOSE International Symposium, 28*(1), 1608-1625.

Leveson, N. (2015). A Systems Approach to Risk Management through Leading Safety Indicators. *Reliability Engineering* and *System Safety, 134*, 17-34.

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

Leveson, N., and Thomas, J. P. (2018). *STPA H*and*book.* Cambridge, MA: Partnership for Systems Approaches to Safety and Security .

Long, D. (2018, June 8). *"MIT was Right--Focusing on EoS Rather than SE.* Retrieved from ViTechCorp.com: http://community.vitechcorp.com/index.php/mit-was-right-focusing-on-eos-rather-than-se.aspx

Marais, K. (2005). *A New Approach to Risk Analysis with a Focus on Organizational Risk Factors.* Cambridge, MA: Massachussets Institute of Technology, Dissertation.

McFarlane, P., and Hills, M. (2013). Developing immunity to flight security risk: prospective benefit from considering aviation security as a socio-technical eco-system. *Journal of transportation Security, 6*, 221-234.

*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. **SAND-PEER REVIEW.**

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.

National Research Council, Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety. (1997). *Digital instrumentation* and *control systems in nuclear power plants: safety* and *reliability issues.* Washington, D.C.: National Academies Press.

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

Orlikowski, W. J. (2000). Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations. *Orginization Science, 11*(4), 404-428.

Pawlicki, T., Samost, A., Brown, D., Manger, R., Kim, G.-Y., and Leveson, N. (2016). Application of Systems and Control Theory-Based Hazard Analysis to Radiation Oncology. *Journal of Medical Physics, 43*(3), 1514-1530.

Placke, S., Thomas, J., and Suo, D. (2015). *Integration of Multiple Active Safety Systems Using STPA SAE Technical Paper 2015-01-0277.* SAE.

Rasmussen, J. (1979). *On the Structure of Knowledge - A Morphology of Mental Models in a Man-Machine System Context (RISO-M-2191).* Roskilde, Denmark: Riso National Laboratory.

Robbins, S. P. (1990). *Organization Theory: Structures, Designs,* and *Applications* (3rd ed.). Prentice Hall.

Robey, D., and Rodriquez-Diaz, A. (1989). The Organizational and Cultural Context of Systems Implementation: Case Experience from Latin America. *Information* and *Management, 17*, 229-239.

Ross, R., McEvilley, M., and Oren, J. C. (2016). *Systems Security Engineering: Considerations for a Multidisciplinary Appraoch in the Engineering of Trustworthy Security Systems (NIST Special Publication 800-160).* Gaithersburg, MD: National Institute of Standards and Technology.

Schultze, U., and Orlikowski, W. J. (2004). A Practice Perspective on Technology-Mediated Network Relations: The Use of Internet-Based Self-Serve Technologies. *Information Systems Research, 15*(1), 87-106.

Silitto, H., Griego, R., Arnold, E., Dori, D., Martin, J., McKinney, D., . . . Jackson, S. (2018). What do we mean by "system"?–System Beliefs and Worldviews in the INCOSE Community. *INCOSE International Symposium, 28*(1), 1190-1206.

Stringfellow, M. V. (2010). *Accident Analysis* and *Hazard Analysis for Human* and *Organizational Factors.* Cambridge, MA: Massachussets Institute of Technology, Dissertation.

*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. **SAND-PEER REVIEW.**

Sussman, J. M. (2014). *The CLIOS Process: Special Edition for the East Japan Railway Company.* Cambridge, MA: Massachusetts Institute of Technology.

Von Bertalanffy, L. (1950). The theory of open systems in physics and biology. *Science, 111*(2872), 23-29.

Von Bertalanffy, L. (1972). The history and status of general systems theory. *Academy of Managment Journal, 15*(4), 407-426.

Waldrop, M. M. (2016). More than Moore. *Nature, 530*(7589), 144-147.

Weaver, W. (1948). Science and Complexity. *American Scientist, 36*(4), 536-544.

Williams, A. D. (2013). System Security: Rethinking Security for Facilities with Nuclear Materials. *Proceedings of the Risk Management for Complex Socio-technical Systems*, (in press).

Williams, A. D. (2015). Beyond a Series of Security Nets: Applying STAMP and STPA to Port Security. *Journal of Transportation Security, 8*(3-4), 139-157.

Williams, A. D. (2018). Beyond Gates, Guards, and Guns: The Systems-Theoretic Framework for Security of Nuclear Facilities. *PhD Dissertation*. Cambridge, MA: Massachusetts Institute of Technology.

Young, W. E. (2015, December). A System-Theoretic Security Analysis Methodology for Assuring Complex Operations Aginst Cyber Disruptions. *PhD Dissertation*. Massachusetts Institute of Technology.

Young, W., and Leveson, N. (2014). An Integrated Approach to Safety and Security Based on Systems Theory. *Communications of the ACM, 57*(2), 31-35.

*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. **SAND-PEER REVIEW.**