Capturing Human, Social & Organizational Influences on Nuclear Security: System-Theoretic Assumption Guided Evaluation (STAGE)*

A. Williams[1]

[1]Sandia National Laboratories*, Albuquerque, New Mexico, U.S.

E-mail contact of main author: adwilli@sandia.gov

Abstract. Recent high profile events at nuclear facilities and common discourse in the professional realm suggest that security vulnerabilities at nuclear facilities seem to be more related to social, organizational or operational influences than technological ones. More specifically, a 2010 report by the U.S. National Academy of Science entitled 'Understanding and Managing Risk in Security Systems for the DOE Nuclear Weapons Complex' concluded that most current risk-based 'methodologies cannot address cultural or organizational barriers to improved security.' While recent efforts to raise the profile of nuclear security culture (e.g., but the International Atomic Energy Agency) or governance (e.g., by the World Institute for Nuclear Security) have generated a useful framework for addressing some of these factors, current analytical techniques struggle to incorporate the effect of such specific (and observed) influences of decreasing security budgets or prioritizing production over security on creating vulnerabilities within nuclear facilities. This suggests a need for nuclear security analysis techniques to move away from such dualistic (and often disparate) analytical frameworks and toward a new paradigm that incorporates both social and technological issues.

In response, System-Theoretic Assumption Guided Evaluation (STAGE) is offered as a framework to identify how social, human and organizational factors influence the vulnerability of nuclear facilities. STAGE evaluates the interaction of performance reliability assumptions, design decisions, implementation realities and daily work routines, practices and behaviors to reframe security as an emergent system of nuclear facilities. STAGE, then, offers an improvement for security analysis by systematically challenging assumptions underlying security design to identify organizational (or social) sources of vulnerabilities to nuclear security. To demonstrate, this paper describes the ability of STAGE to evaluate security vulnerabilities related to international spent nuclear fuel (SNF) transportation. In contrast to traditional approaches to SNF transportation security that build off of decades of SNF transportation safety analysis, which focus technical cask design, acceptable dose rates, defense-in-depth systems and probabilistic hazard estimates, STAGE evaluate this transborder, multi-modal distributed process by including such non-traditional security influences as ensuring consistent security across countries with varying resources and adequately shifting security responsibilities among federal and local organizations along a transportation route.

The results of comparing security approaches to a hypothetical international SNF transportation demonstrate that STAGE is able to rigorously identify organizational influences on the ability of a nuclear facility to achieve its security functions and suggests that its inclusion as an analytical tool can improve nuclear security. Despite today's increasingly complex security environment, STAGE offers a method for identifying and managing underlying assumptions to improve the security of nuclear materials across the nuclear fuel cycle.

Key Words: Nuclear security; Organizational influences; Transportation security; Nuclear security culture.

1. Introduction

Despite many positive strides in nuclear security, recent events at nuclear facilities and common knowledge in the professional realm suggest that security vulnerabilities at nuclear facilities seem to be more related to organizational or operational influences than technological ones. Current approaches to evaluating nuclear security struggle to explicitly explain the effect of organizational factors on the completion of core security functions—which supports the claim by the World Institute for Nuclear Security (WINS), 'An organization may be technically competent while remaining vulnerable if it discounts the role of the human factor.' [1, This insight is supported by the historical evolution of security

through an interesting mix of technological development, borrowing best practices, national sovereignty and international politics.

Through the 1960s, security emphasized classifying information and strategically locating stores of special nuclear material (SNM). In the 1970s Congress charged Sandia National Laboratories (SNL) to be the lead laboratory for developing security technologies and methodologies for Department of Energy (DOE) nuclear facilities, including an emphasis on 'diversion path analysis,' wherein event and fault trees were employed to identify the most vulnerable pathways. In the 1980s, nuclear security focused on performance-based evaluation and establishing a 'generic threat statement' to standardize security designs and technologies. The early 1990s saw nuclear security evolve around the design basis threat (DBT), which resulted in an increasing use of computer-based simulation and analysis tools for calculating the probability an adversary will be interrupted on a particular path and the probability an adversary force will be defeated by a response force.[2] Starting in the early 2000s, the emphasis of nuclear security shifted toward counter-terrorism strategies, including the need to protect against suicide bombers and large-scale attack teams.[3]

As suggested by its historical evolution, nuclear security must continually adapt both to new and increasing potential adversary capabilities, but also to changing operational contexts, organizational environments and geopolitical pressures. However, traditional approaches to designing and evaluating nuclear security have emphasized technological solutions (e.g., [4], [5]) to minimize vulnerabilities, while more recent approaches have highlighted the importance of cultural (e.g., [6]) and governance issues (e.g., [7]). More specifically, a 2010 report by the U.S. National Academy of Science entitled 'Understanding and Managing Risk in Security Systems for the DOE Nuclear Weapons Complex' concluded that most current risk-based 'methodologies cannot address cultural or organizational barriers to improved security.'[8]

Recent trends toward leveraging experiences and lessons from safety culture to security are limited by the inherent tension between the openness and transparency of the former and focus on information protection and adversary awareness of the latter.[9] Here, efforts to invoke security culture to improve on currently accepted best practices in nuclear security struggle to account for the 'human factor' relates to traditional metrics of security, as suggested in one assessment of the success of applying the International Atomic Energy Agency's (IAEA) nuclear security culture model in a developing nuclear country that noted

> While the IAEA has released methodologies on evaluating vulnerabilities and physical protection, it has not yet introduced guidelines on assessing the human factor in detection, delay, and response.[10, p. 40]

This paper introduces a new security analysis approach intended to explicitly link the influence of organizational factors (e.g., one element of the 'human factor') to traditional security system metrics of detect, delay and respond. In this manner, this new approach seeks to account for the fact that while 'Most of the focus on physical protection is on systems…it takes people to design, install, operate, test and repair the systems properly.'[9, p.30-31]

2. STAGE: System-Theoretic Assumption Guided Evaluation

According to nuclear security expert General (ret.) C. Donald Alston,

> Culture does not exist in a static environment, and there are pressures, both positive and negative, at all times. Organizations…need to…control and influence the factors that create a culture enabling mission success everyday.[9, p.61]

In response, System-Theoretic Assumption Guided Evaluation (STAGE) is offered as a rigorous framework to identify how organizational factors influence the security performance of nuclear facilities. Related to recent work in system security engineering [11], STAGE defines nuclear facilities as systems composed of interrelated components that maintain dynamic equilibrium through information and control feedback loops that allow it to adapt to changes in itself (or its environment) to achieve its objective. STAGE evaluates security as an emergent property by analyzing how organizational influences (e.g., leadership) and factors (e.g., resources and policies) influence a security system's ability to achieve detection, delay and response performance requirements.

More succinctly, STAGE argues that security performance emerges from the interaction of technological elements and organizational influences (Fig. 1). This suggests that security is more than defense-in-depth, balanced protection or performance test based arrangements of technical components ([4], [5]) and must consider how closely the actual operational environment matches the expected operational environment. The larger the difference between expected (e.g., design) and experienced (e.g., actions and feedback) operational environment, the less able the security system is able to achieve security performance for which it was designed—representing a source of potential vulnerable security systems at nuclear facilities.

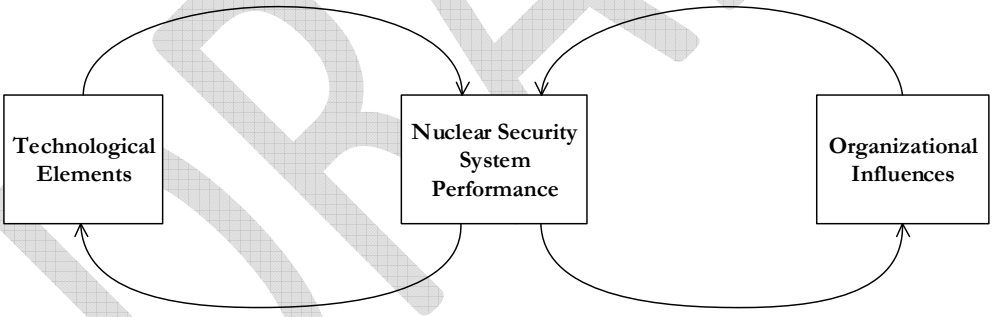

Figure 1. Socio-technical model of security as an emergent system property.

Per the quote from General Alston above, one way to address these vulnerabilities (e.g., achieve security system mission success) emerges from how well nuclear facilities can control organizational influences on the operational environment. Nuclear security system design includes down-selecting, arranging and locating technological security components, as well as assumptions regarding the operational environment in which the security system is expected to achieved desired performance requirements. Organization science [12] offers a model that describes how such organizational influences can reinforce or oppose the use of technological components by security personnel to complete security-related work tasks in support of security system performance requirements.

The operational environment can be described in terms of organizational influences under the control of the nuclear facility (called 'institutional properties') that must be present in order to support the capability of security personnel to complete security-related work tasks. Recent

literature from system safety [13] provides a set of organizational and managerial assumption categories (e.g., operational procedures, coordination and cultural) that help define these institutional properties to support desired security system performance outcomes. These categories can be used to determine institutional properties necessary for nuclear facilities to provide in order to align operational realities with the expected operational environment (undergirding security system design) and achieve desired security system performance. In this sense, STAGE captures the missing 'human factor' and expands the solution space for improving nuclear security.

Defining the operational environment as a set of institutional properties that support the capability for individual security personnel to complete security-related work tasks, builds on the recent emphasis on nuclear security culture ([1], [6]) and governance to improve nuclear security.[7] These two approaches offer lists of organizational influences identified by a range of nuclear security professionals, practitioners and experts to help explain the differences between expected and experiences security system performance. While these influences are a good start, STAGE explicitly identifies the causal relationships between related institutional properties, individual capability to complete security-related work tasks and security system performance. STAGE, then, represents a logical path between institutional properties (e.g., organizational influences under the control of a nuclear facility) and security system performance—offering an analytical capability include how organizational influences may violate security system performance expectations.

For some technological security components, the potential for institutional properties to violate related performance expectations will be limited—the ability of 0.5-meter-thick wall of an underground storage vault to provide delay, for example. For others, though, institutional properties will present greater opportunities to violate performance expectations—the probability of detection of an emergency exit door, for example. As such, STAGE analyses system security performance as a function of both technological security system effectiveness and the ability of a nuclear facility to provide the necessary institutional properties that support completion of security-related work tasks.

3. Analysis & Discussion

Consider the following hypothetical case description as an example of the increased complexity facing the security of multi-modal and multi-country spent nuclear fuel (SNF) shipments.[1] Country C, host to the SNF disposal site, has a stable government with low levels of corruption; a strong rail, air, road and maritime transportation infrastructure; and, poses a low safeguards risk. Similarly, Country A, host to facilities generating SNF, has a stable government and a strong rail, air, road and maritime transportation infrastructure, but also has moderate levels of corruption and terrorist network activity in-country and along its borders. Lastly, Country B—which separates our two nuclear capable nations—is undergoing civil unrest after a military coup and governmental takeover. Though its transportation infrastructure (primarily roads) is in great disrepair, local law enforcement is unreliable and corruption is rampant, governance along the coast is considered more stable

[1] Though limited in number, past experiences (e.g., [14], [15]) and the predicted significant increase in international SNF transportation (e.g., SNF 'take-back' agreements being offered by nuclear fuel suppliers to support the increased global demand for nuclear power) suggest the need for security analysis able to evaluate the expanding complexities of securing SNF during global transit.

than that inland. The SNF generated in Country A consists of 50 GWd/tU[2] has was removed from a pressurized water reactor and has been sitting in wet storage at Site A for 50 years. As such, this SNF will be transported in an IAEA-compliant, type B cask (e.g., similar to the AREVA TN cask series). The overall goal of this case is for SNF to travel from Country A to the disposal site in Country C, according to this high level route description:

- SNF cask is loaded in Country A onto a rail car for transporation to the Port of Country A where it is loaded onto a barge;
- SNF cask travels via international waters to the Port of Country B in the northwest corner of the country and loaded onto a truck; and,
- SNF cask travels by road through western Country B, across the border and across interior Country C to the disposal site.

This hypothetical route was selected amidst a set of security-related factors, including the desire to avoid the greater political instability and terrorist activity of interior Country B and the recent issues with piracy along the southern Country B coast. For more details on the casks design and specific route details, please see [16]. To focus the scope of the analysis, consider the scenario in which the transfer of security responsibilities from Country B officials to Country C officials when the SNF transportation truck crosses the border. Here, the scenario describes a 'state' inclusive of insights provided by the World Nuclear Transport Institute (WNTI) and the World Institute for Nuclear Security (WINS) (e.g., coordination of security responsibilities between entities along the route and at points of transfer).

Consider, for example, locking tie-down mechanisms used to secure the cask to its transportation vehicle and increase the time required for unauthorized access of the cask (e.g., increase delay time). STAGE argues that this security performance requirement is achieved when individual users are able to complete the related work task of attaching (or verifying the attachment of) the locking tie-down mechanisms to the transportation vehicle. While a seemingly straightforward task, the process for attaching (or verifying the attachment) of the locking tie-down mechanism may change if the transportation vehicle is a truck, railcar or barge—each of which are used on this hypothetical route. Further, each potential individual with the responsibility to either attach or verify the attachment of the locking tie-down mechanisms must have certain capabilities—which includes ensuring the required level of knowledge to do so is defined and communicated; the organizational capabilities necessary to do so are known and provided; that organizational conventions/rules define doing so as 'sanctioned' behaviour; and, that users and management have a shared level of knowledge of system performance. These capabilities, then, determine institutional properties necessary to be provided by the nuclear-related organizations along the transportation route to ensure that the desired increase in delay is achieved.

Per STAGE, it is necessary to identify who and/or how the institutional properties are provided. This suggests that even though the same technology (e.g., locking tie-down mechanism) that is employed in different operational environments requires the same institutional properties, they will likely be delivered in different manners. For example, the level of knowledge required to properly attach (or verify) the locking tie-down mechanisms would be provided in regular training given by the robust competent security authority of Country A and Country C. Country B, however, does not have a robust nuclear infrastructure

[2] These units, Gigawatt-days per ton of enriched Uranium, is a descriptor of how nuclear material is used within a given power reactor.

and thus may not have the ability to provide the necessary level of knowledge to complete this task. STAGE, then, identifies a potential vulnerability in the overall security of this transportation case—but also identifies a specific area wherein security can be improved. As indicated, the analytical goal is for nuclear facilities to provide the institutional properties necessary to support the capability for individuals to complete security-related work tasks enabled by security system design.

4. Summary & Conclusions

The results of a hypothetical international SNF transportation demonstrate that STAGE is able to rigorously identify organizational influences on the ability of a nuclear facility's security system to achieve its expected performance. By emphasizing individual capability (e.g., enabling user ability to complete work tasks) versus intentionality (e.g., managing personal intent) or probability (e.g., assuming stochastic human behaviour), this systems-level approach expands the solution space for security designers, analysts and decision-makers. As indicated in Fig. 1, by explicitly linking operational environment and security system design, STAGE provides additional avenues for improving security system performance. STAGE also accounts for new sources of security system vulnerability, namely those that arise from how facility personnel interact with the technological system components. STAGE fills a gap between the technical, physical protection focus of traditional nuclear security analysis (e.g., DEPO) and the recent emphasis on nuclear security culture and governance—extending the analytical capabilities of both, as summarized in Table 1.

Table 1. Comparison of organizational factors in nuclear security analysis approaches

	DEPO (ITC)	**IAEA Nuclear Security Culture**	**WINS Nuclear Security Governance**	**STAGE**
Definition of security	Probabilistic ability of PPS components to detect, delay and respond to adversaries along predetermined paths	Prevention, detection & response to, malicious acts (theft, sabotage) involving nuclear/ radioactive materials or facilities	Governing to ensure the effective application of security measures to mitigate threats within the operational environment	Emergent property of interacting organizational & technical components within a 'systems' perspective of a nuclear facility
Treatment of Organizational Factors	As one time probabilities of human error	As factors for self-assessment in the IAEA nuclear security culture model	In terms of hierarchical management structures and responsibilities	As controllable, dynamic influences on user capability to complete work tasks undergirding security system design

Security Improvements are	Technical 'add-ons' to already operating nuclear facility security systems	Tangible & intangible actions taken to reinforce that a credible threat exists & that security is important	Based on inter-related voluntary, mandatory and regulated policies, procedures and decisions	Considered as both technical & organizational improvements to enable completion of work tasks to meet desired security performance

As nuclear facilities become more multinational and nuclear operations more globalized, operational environments for security systems will become more complex—necessitating new approaches for maintaining progress in securing nuclear materials and facilities. Despite today's increasingly complex security realities, STAGE offers a method for identifying organizational influences that underlay security system assumptions to improve the security of nuclear materials across the nuclear fuel cycle.

5. References

[1] WORLD INSTITUTE FOR NUCLEAR SECURITY, Nuclear Security Culture: WINS International Best Practice Guide (Rev. 3), **1.4**, Vienna (2016).

[2] DESMOND, W., et. al., "The First Fifty Years: A Review of the Department of Energy Domestic Safeguards and Security Program", J. of Nucl. Materials Mgmt, **26(2)** (1998).

[3] ROSANO, R. (July 2013). "Developing Security Strategies for Alternative Nuclear Designs", IAEA-CN-203 (Proc. IAEA Conf. Nuclear Security Vienna, 2013).

[4] GARCIA, M.,. Vulnerability Assessment of Physical Protection Systems, Butterworth-Heineman, Boston (2005).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Revision 5, Vienna (2011).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture Implementing Guide, Nuclear Security Series No. 7, Vienna (2008).

[7] WORLD INSTITUDE FOR NUCLEAR SECURITY, Security Governance: International Best Practice Guide, **1.3**, Vienna (2010).

[8] COMMITTEE ON RISK-BASED APPROACHES FOR SECURING THE DOE NUCLEAR WEAPONS COMPLEX, Understanding and Managing Risk in Security Systems for the DOE Nuclear Weapons Complex, Nat'l Acad. Press, Wash., DC (2011).

[9] RUSEK, B., et. al., Brazil-U.S. Workshop on Strengthening the Culture of Nuclear Safety and Security: Summary of a Workshop, Nat'l Acad. Press, Wash., D.C. (2015).

[10] KHRIPUNOV, I., The Human Dimension of Security for Radioactive Sources: From Awareness to Culture, Univ.of Georgia Center for Int'l Trade & Security, Athens, GA (2014).

[11] ROSS, R., et. al., Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, Special Pub. 800-160: Second Public Draft, Nat'l Institute of Standards and Tech., Gaithersburg, MD (2016).

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

[13] LEVESON, N., "A Systems Approach to Risk Management Through Leading Safety Indicators,' Reliability Engineering & System Safety, **136** (2015) 17-34.

[14] MUNERA, H., et. al., "Risk associated with transportation of spent nuclear fuel under demanding security constraints: The Colombian experience", Risk Analysis, **17(3)** (1997) 381-389.

[15] IMAN, K., et. al., RRSNF Shipment Operation of Indonesian Research Reactors, Return of Research Reactor Spent Fuel to the Country of Origin: Requirements for Technical & Adminstrative Preparations & National Experiences, (Proc. of IAEATech. Mttg. Vienna 2008) 109-119.

[16] WILLIAMS, A., et. al., "Preliminary Results from a System-Theoretic Framework for Mitigating Complex Risks in International Transport of Spent Nuclear Fuel", INMM 2016, (Proc. Annual Mttg. Atlanta, GA., 2016).