SAND2022-3642J

Revisiting Current Paradigms: Subject Matter Expert Views on High Consequence Facility Security Assessments

T. Gunda, S. Caskey, A. D. Williams, G. C. Birch
Sandia National Laboratories, Albuquerque, NM, USA, [tgunda; sacaske; adwilli; gcbirch]@sandia.gov*

Abstract

Security assessments support decision-makers' ability to evaluate current capabilities of high consequence facilities (HCF) to respond to possible attacks. However, increasing complexity of today's operational environment requires a critical review of traditional approaches to ensure that implemented assessments are providing relevant and timely insights into security of HCFs. Using interviews and focus groups with diverse subject matter experts (SMEs), this study evaluated the current state of security assessments and identified opportunities to achieve a more "ideal" state. The SME-based data underscored the value of a systems approach for understanding the impacts of changing operational designs and contexts (as well as cultural influences) on security to address methodological shortcomings of traditional assessment processes. These findings can be used to inform the development of new approaches to HCF security assessments that are able to more accurately reflect changing operational environments and effectively mitigate concerns arising from new adversary capabilities.

Introduction

Securing high consequence facilities (HCFs) ─ which are defined as those whose incapacitation would have a devastating impact on national security, economic prosperity, and/or public health [1]─ is subject to a range of 21st century challenges, including the need to coordinate governance, network architectures, wide-area situational awareness, forensics, learning, and trust management [2]. Additionally, two observable trends are particularly troublesome. The first is the continuing evolution of threats to HCFs, exemplified by the recent attacks on Saudi Arabian oil facilities by rebels using unmanned aerial systems (UAS) [3], cyberattack at the Kudankulam nuclear power plant in India [4], and the increasing frequency of insider attacks [5] [6]. The second relates to how HCF operational activities themselves are also changing, for example, through increased digitization or being located in remote areas [7]. Taken together, these trends challenge both the efficacy and effectiveness of current paradigms for security assessment of HCFs.

HCF operations follow lifecycles that consist of varying combinations of producing, storing, using, changing, and destroying (potentially) sensitive assets, including nuclear, chemical, biologic, and radiologic materials. In addition to the materials themselves, sensitive assets also encompass equipment and documents, whose loss or misuse could cause significant social, political, and/or financial disruptions. The security posture at HCFs, thus, focuses on the "prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts" involving high consequences assets [8] [9] [10]. Security assessments are an important risk reduction strategy that provide performance-based insights regarding the current capabilities of an HCF to respond to possible attacks [11].

Multiple processes and evaluation tools have been developed to provide an analytical basis for security assessments [12]. For example, the Design Evaluation and Process Outline (DEPO) process leverages probabilistic risk assessment philosophy in nuclear safety to evaluate the probability of interdiction of an adversary based upon the principles of detection, delay, and response [13] [14] [15]. Other more recent work has sought to expand these approaches to incorporate heuristic-informed simulations [16] and Bayesian updating to better address dynamic parameters [17]. Alternate HCF security assessments range from use of semi-quantitative risk matrices [18] to regulation-based approaches [19] and comparisons for "weakest link" using risk-informed assessments [20].

Researchers have noted, however, that these approaches struggle to account for the increasing complexity and changing characteristics observed in current security operations [13] [19] [21]. The increasing pace of technological, organizational, and societal change necessitates a critical

review of security assessments to ensure they continue to meet intended risk reduction objectives for HCFs. Others have specifically identified how characteristics of structural (e.g., heterogeneity and interdependence) and dynamic (e.g., emergence and adaptive learning) complexity directly challenge fundamental understanding of vulnerability and risk analysis [22]. In response, this research focuses on better understanding the current state of security and identifying specific opportunities to support the transition toward a more "ideal" future state. This work seeks to understand these states of security by capturing and evaluating a range of HCF security-related perspectives. These perspectives include (but are not limited to) HCF security operations, vulnerability analysis, human cognition, and HCF resilience analysis. Such perspectives can provide a more comprehensive and contextualized understanding of the following research questions:

1. How does the current state of security assessments mitigate increasingly complex challenges?
2. How does HCF security need to evolve to achieve and maintain an "ideal" state of performance amidst such increasingly complex challenges?

Given the multiple components (physical, cyber, and human) and nonlinear feedbacks and interactions commonly experienced in HCFs [23] [24], this research adopts a systems approach for analysis [25]. Insights from such a systems-based approach can help coordinate the multiple perspectives necessary to better understand the influence of HCF mission and design (as well as actual implementation) on security assessments—including addressing new vulnerabilities emerging from infrastructural dependencies [26]. In the following sections, the mechanisms for data collection and methods for evaluation are described, including the construction of a systems-based force field diagram (FFD) to illustrate the influence of the identified factors on either driving or inhibiting progress towards the ideal state of security [27]. The insights from this study establishes a foundation of needs and is informing the development of new and modified approaches (such as multi-layered networks) that better address critical gaps within HCF security assessment methodologies.

Methods

Data Collection

Given the complexity of HCF security activities, two factors influenced our data collection. The first considered diverse perspectives required to understand the current state of and future opportunities for HCF security assessment. The second related to robust and explicit capture of context, dynamics, and nuances within qualitative insights about HCF security activities [28]. Interviews have been shown to provide useful insights for comparing perspectives between operators with similar job tasks from different companies [29], to deepen understanding of complex system functions [30], and to validate critical infrastructure simulation outputs [31]. As a result, this analysis used interviews and focus groups (FGs) for data collection that targeted HCF security professionals across a range of expertise, including security engineering, technology development, operations, and system analysis as well as resilience analysis and human cognition.

To address the research questions, the qualitative data collection probed perceptions of the current state of security assessments, strengths and weaknesses of current HCF-related security approaches, and depictions of ideal future states for HCF security. A semi-structured approach guided by pre-determined, open-ended questions was used to elicit SME responses [28]. Semi-structured methods have the advantage of being flexible enough to capture the diverse perspectives and details shared by the various SMEs, whether it be through interviews or FGs [32]. Interviews focus on soliciting responses from a single SME while the design of FGs allows interaction between participating SMEs leading to "discussion [that] builds on the group dynamics to explore the issues in context, depth and detail" [33, p. 29]. A list of pre-determined questions tailored to guide the interviews and focus groups is provided in Table 1.

In total, 29 SMEs from across Sandia's various HCF security-related mission areas were consulted, through 18 interviews and 2 FGs (comprising of 11 participants) between December 2019 and March 2020 (Table 2). The FGs were organized into two groups, one focused on

integrated assessment professionals in security operations (4 participants) and the other on early career HCF security professionals with 1-5 years of work experience (7 participants). Most of the interviews (16 of 18) and both FGs were conducted in person; two interviews were conducted via telephone. A formal review was submitted to and approved by Sandia National Laboratories' Human Studies Board (ID # SNL000266).

Table 1. Open-Ended Questions used to Guide Interviews and Focus Groups.

Topic	Guiding Questions
Demographics	How do you describe your current and/or past-role(s) in HCF security activities? How long have you been in this role?
	How were you introduced to this area? What training have you received in this area?
Current State	How would you describe the current state of HCF security assessment?
	What factors influence the actual implementation of HCF security assessments?
Future State	What is your vision of the *ideal* HCF state of security?
	What do you see as the necessary outcome for future HCF security assessments?
Resources	What methods and metrics are used for evaluating effectiveness of HCF security within assessments?
	Are there relevant case studies or perspectives that should be incorporated into HCF security?

On average, each interview or focus group lasted between 45 and 75 minutes and included at least two members from the research team to capture notes (either typed or hand-written). Each discussion began by reviewing the consent document and introducing the overall research goals before initiating an SME-driven conversation. During these discussions, research team members also asked clarifying questions to gain additional insights from interviewee responses to pre-determined questions (e.g., "Can you expand on …?" or "Can you provide a specific example of …?"). Immediately after each discussion, the team members reviewed the transcribed notes to fill in any gaps and created a single report capturing key insights, anecdotes, and quotes. In addition to describing states of security, each SME was asked to name other security professionals who could provide useful insights to support these research objectives. This snowball sampling approach helped ensure that relevant perspectives were being sufficiently represented within the analysis [34]. No additional interviews and FGs were scheduled once SME discussions stopped revealing new insights, indicating the data collection reached a saturation of themes [35].

Data Analysis

The qualitative data were analysed using interviewee quotes and anecdotes to identify patterns that focused on the interpretation and integration of insights shared by the SMEs [23]. Data about the current state of security were reviewed and grouped into common themes to evaluate the impact of both commonalities and outliers in the information shared across SMEs. Identification of themes was conducted by two independent coders, whose results were then cross compared; the categorization of themes had a 90% agreement between the two encoders, indicating a high level of agreement in interrater reliability [36].

Shared insights are influenced by the specific perspectives and experiences of the SMEs. For example, consider an SME involved in HCF security operations who is privy to long-standing oversights within nuclear facility assessments. Such an SME might be more aware of how findings from vulnerability assessments (VA) are integrated into subsequent decision-making than an SME who has been only involved in conducting the VAs themselves. While such biases could be introduced into analysis by virtue of the representative nature of the SMEs contributing to the data, these biases also represent variations in understanding that provide opportunities to gain a richer evaluation of the data. To evaluate and account for the influence of these

variations on shared insights, the data were analysed according to common models of HCF security philosophy and practice (i.e., worldviews [37]); the type of HCF security training; and, years of HCF security-related service (Table 2). Categorizing SMEs according to "worldviews" leverages systems engineering approaches to leverage key insights from SMEs across different areas of expertise and better address current challenges to HCF security [37].

The SMEs were grouped into three HCF security worldviews: 1) traditional security, 2) emerging security, and 3) systems analysis. SMEs classified as "traditional security" included any individuals that are involved in execution of security analysis or designs domestically or internationally, which ranged from analysis to management activities. SMEs categorized as "emerging security", on the other hand, were primarily involved in developing new tools, technologies, or paradigms within the HCF security realm (including cybersecurity). It is interesting to note that most of the SMEs with the emerging security worldview have experience implementing current HCF approaches. Finally, SMEs categorized as "systems analysis" shared a common perspective of employing systems-based approaches and formal analytical backgrounds despite working in such diverse HCF-related applications as resilience, human cognition, and security analysis. The use of worldviews helped capture the influence of diverse (or hybrid) career paths on an SME's perspective instead of just relying on the perspective of their current role. For example, an SME that implemented security, conducted security assessments, and now teaches security assessments was categorized as having a "traditional security" worldview whereas an SME that conducted security assessments, questioned the underlying logic of current approaches, developed new HCF security-related approaches, and continues to develop new approaches was categorized under the "emerging security" worldview.

Table 2. Worldviews and Demographics of SMEs Consulted for Analysis.

ID*	World View**	Area of expertise	HCF Training***	Years of Expertise
A	TS	Vulnerability analyses; former protective force officer	F	>10
B	TS	Security assessments at HCF	F	>10
C	ES	Modelling & simulation of HCF security	I	>2
D	TS	Former security officer at HCF	I	>10
E	SA	Resilience frameworks & systems analysis	I	>6
F	SA	Modelling of physical security activities	F	>2
G	ES	Physical security requirements at HCF	I	>5
H	ES	Security assessments at HCF	F	>10
I	ES	HCF modelling & simulation analysis	F	>5
J	SA	Threat & consequence analysis	I	>10
K	ES	Emerging security/foundational security background	F	>20
L	ES	Intelligence community-related security/physical security	I	>10
M	TS	Evaluation of security assessments at HCF	F	>30
N	SA	Human-machine interactions	I	>10
O	TS	Vulnerability analyses; former protective force officer	I	>30
P	SA	Risk analysis & associated principles	F	>15
Q	SA	Evaluation & performance testing of HCF security	I	>5
R	TS	HCF safety & security analysis	I	>5
FG1	SA	Integrated & strategic analyses at HCFs	I	2-30
FG2	TS	HCF physical security, support security implementation	I	2-7

***Single letters indicate one-on-one SME interviews while "FG#" indicates a focus group**
****TS = traditional security, ES = emerging security, and SA = systems analysis**
*****F = formal, I =informal**

Categorization of SMEs into worldviews followed a similar approach with cross-comparison of two independent coders' results; there was 100% agreement in the coders' categorization of SMEs into worldviews [36]. The extent to which SMEs (from diverse domains) contributed to common themes and metrics was then evaluated to determine the robustness and validity of observed patterns and themes in the data. Training and years of experience were also used to

evaluate the generalizability of the patterns between worldviews and resulting themes. Themes were identified by identifying similarities between quotes and anecdotes in the data.

In addition to categorization into common themes, the dominant factors influencing the state of security (as noted by SMEs) were translated into a force field diagram (FFD) [27]. An FFD is based on the concept of countervailing forces influencing overall system (e.g., state of security) behaviour. Specifically, the role of each force (i.e., factor) and the relative levels of influence were captured from the data to describe how they either drove overall behaviour relative towards the ideal state or inhibited change [27]. The number of SMEs that discussed a factor as well as the polarity of the SME language guided FFD construction. For example, if two SMEs indicate that current technology investments disincentivize revisiting current HCF approaches while 10 SMEs indicate technology advancements motivate revisiting current approaches, then the arrow for a “driving force” toward revisiting current HCF approaches would be much greater than the “inhibiting force” arrow. Similarly, if SMEs indicate that policy considerations overwhelm technology considerations, then the relative magnitude of the arrows for policy would be greater than for technology considerations. Through its visualization approach, the FFD facilitates systems-level understanding of the diverse factors influence the state of security at any given time.

Results

The SMEs consulted were evenly distributed between the traditional security (7), emerging security (6), and systems analysis (7) worldviews (Table 2 and Figure A1). More SMEs fell into the mid- (10-19 years) and early (1-9 years) career categories than the late career (20+ years). The mean years of experience ranged from 14 years for traditional security professionals to 9 years for emerging security and 8 years for systems analysts. There is an even distribution between formal and informal training backgrounds between the three worldviews (Figure A1). Below we summarize common themes identified in the data (including commonalities between worldviews) relating to the current state of security as well as specific opportunities for transitioning toward an ideal state of security. Because of the spread of the data across worldviews and years of experience, the subsequent trend analysis and insights on current capabilities, future needs, and ideal states of HCF security indicated observed themes are reliable, valid, and generalizable.

Current State: Common Themes

Three common themes related to current and future states of security were observed in the data: 1) changing operational designs and contexts, 2) methodological shortcomings, and 3) cultural influences. The changing operational designs and contexts theme focused on spatiotemporal variations of HCF security investments, namely whether past investments continue to operate and meet current performance needs, as well as the transferability of HCF security performance across different locations. The methodological shortcomings theme concentrated on issues with specific analytical approaches for conducting HCF security assessments. Finally, the cultural influences theme captured institutional and attitudinal factors that impact HCF security activities.

Sankey diagrams, which can visualize quantities of items between features, were used to illustrate the relationships between common themes for the current state of security and HCF worldviews. Generally, all three themes were highlighted by SMEs from all three worldviews, with traditional security professionals being marginally more sensitive to changing operational designs and contexts than the other worldviews (Figure 1). Each of the contextual factors in associated themes have an impact (either driving or inhibiting change) moving HCF security towards a conceptual ideal state. The FFD summarizes these forces and associated levels of that impact (Figure 2). Using this type of comparison between driving and inhibiting factors can support discussions on potentially conflicting factors. Additional details about each of the themes and associated factors shared by SMEs are summarized in the following subsections.

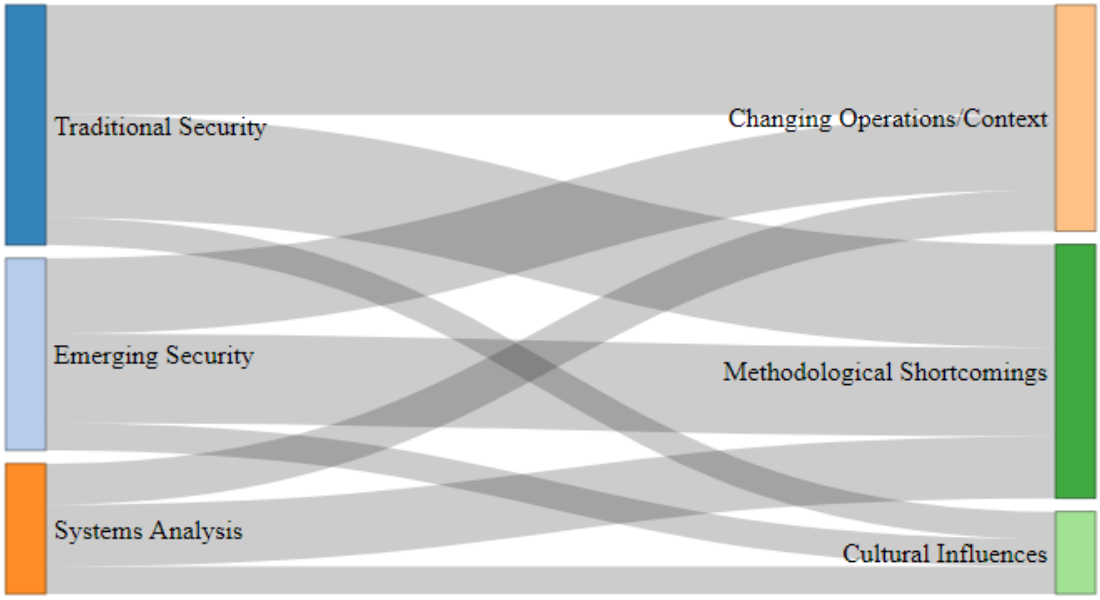


Figure 1. HCF Worldview Sankey Profile of Common Themes for the Current State of Security. Note: Width of the bands indicate importance of theme (right) (based on number of quotes) to a given worldview (right).

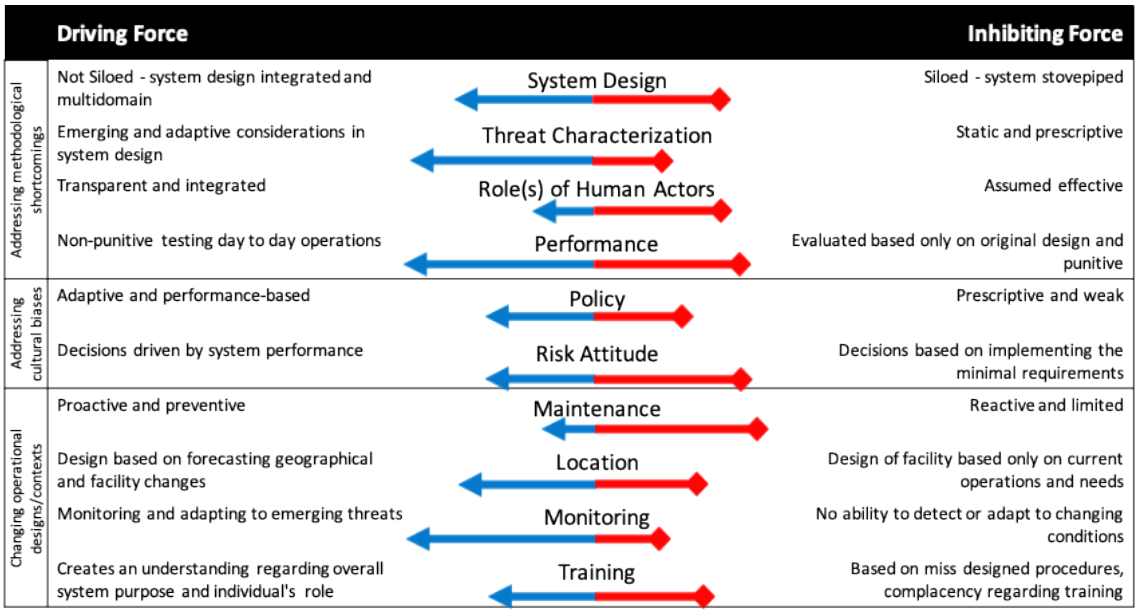


Figure 2. Force Field Diagram of Factors Influencing State of Security. Length of the arrows indicate the strength of the forces to impact change towards the ideal state; arrows going from right to left (blue) are driving towards the ideal state while arrows going from right to left (red) are inhibiting change.

Theme 1: Changing operational designs and contexts

Within this theme, maintenance concerns, differences in HCF types, training needs, and monitoring were discussed by multiple SMEs as impacting the state of security. Maintenance and monitoring items were raised by SMEs from all three worldviews while location and training concerns were highlighted by only the traditional and emerging security professionals (Figure A2).

Maintenance-related concerns were raised by multiple SMEs across worldviews (Figure A2), including [O, D, and FG2] from traditional security; [C and H] from emerging security; and [P, Q, and FG1] from systems analysis. Some SMEs [FG1 and FG2] noted that there is a prevailing assumption that installed systems will continue to operate at designed specifications but inadequate investments in maintenance will lead to increasing gaps, which in turn affect HCF performance capabilities. Other SMEs (including [D, K, L, and Q]) also noted trade-offs associated with human and technological capabilities and associated maintenance. For example, SME [Q] noted that often, the more complicated and complex the introduced HCF security technology, the more maintenance (and resources) is required to ensure the technology continuously operates to meet performance requirements. Whereas for human activities, SME [D] noted that issues of complacency can often emerge with operators conducting routine tasks. Based on the SME insights, maintenance generally acts as an inhibiting force since proactive investments to address gaps to ensure system maintenance are often considered cost-prohibitive (Figure 2).

Three SMEs with the traditional security worldview [A, D, and FG2] and one with emerging security worldview [H] noted challenges arising from implementing current assessment approaches in locations where the local specifications did not match those often assumed in current security assessments. Consider, for example, local HCF security specification differences between a traditional nuclear power facility in the U.S. versus a commercial chemical facility in the U.S. or a nuclear power facility overseas. In non-U.S. nuclear facilities, it is not unusual for security to be considered an afterthought and not as part of the initial facility design. In addition, assumptions regarding personnel roles and responsibilities can vary significantly across HCF domains and geographical facility locations. These anecdotes illustrate how underlying assumptions of the security process greatly influence the design, implementation, and outcomes of the associated assessments. As such, considering the geographical location as part of security enables inclusion of facility changes for ongoing security activities and would serve as a driving force toward an ideal state of security (Figure 2). Conversely, considering only the current state is an inhibiting force since new developments (e.g., housing around a once remote site) would seemingly change only the original security requirements.

Six SMEs (3 from traditional security worldview [A, R, and FG2] and three from emerging security worldview [G, I, and K]) noted training-related deficiencies. SME [R] noted that while there are policy degrees focusing on HCF security, the lack of technical degrees in this domain contributes to the gap in systems thinking applied to HCF security [12]. These challenges become more apparent when considering non-nuclear HCF facilities, such as hospitals, where the personnel are balancing security priorities with their ongoing operations. Most facilities train for HCF security only using prescriptive procedures and often do not perform validation on those procedures. This creates an inhibiting force as individuals can lose an understanding of the details and logic behind the procedures, ultimately becoming complacent in their implementation (Figure 2). Training that promotes understanding behind the procedures and elucidates the purpose of the trainees' security-related role at the HCF represents a driving force the ideal state of security (Figure 2).

Finally, SMEs also highlighted the role of regular monitoring for emerging and evolving adversary threat capabilities. SMEs from traditional security [A, B, D, M, O, R, and FG2], emerging security [G, H, and I], and systems analysis [F, Q, and FG1] each highlighted the constant operational changes resulting from concerns about cyber threats (e.g., denial of service attacks), insider threats, and aerial attacks (e.g., UAS) as well as from the increasing difficulties in protecting soft targets and supply chains (Figure A3). These emerging threats underscore the value of understanding assumptions of current security approaches (and assessments) and what future changes may be necessary. SMEs identified a notable gap in the existence of adequate (and regular) monitoring for emerging and evolving adversary threat capabilities, which represents an inhibiting force on the HCF security performance and adaptation (Figure 2). Having a formalized process for this monitoring can support adaptive and responsive behaviours as a driving force toward the ideal state of security (Figure 2).

Theme 2: Methodological Shortcomings

This second theme manifested as siloed nature of activities, incomplete threat categorization, performance evaluation methods, and inadequate consideration of human (and organizational) factors described in the data. These examples of methodological shortcomings emerged in discussions of both general security activities and security assessments. In contrast to Theme 1, patterns within the methodological shortcomings theme were more consistently identified by SMEs from all three worldviews (Figure A2).

Almost all SMEs (including 6/7 from traditional security, 6/6 from emerging security, and 5/7 from system analysis) highlighted the siloed nature of security activities (including assessments) as a significant issue. Such silos occur across security-related activities, including limited interactions between protection force and facility operations personnel, between site design and site assessment personnel, and between different site security-related operations (e.g., cyber experts and physical site experts). These types of silos seemingly lead to gaps in systemic understanding of security, leading to popular notions of security as "only" about guns, gates, and guards (SMEs [G, J, O, and R]). More pointedly, SME [P] stated that "stovepipes kill us because adversaries do not think in stovepipes." Adoption of a systems approach was recommended by the SMEs across all 3 worldviews, especially given the different ways that emerging risks challenge current security activities. An integrated and multi-domain system is a clear driving force for reaching the ideal state of security. In contrast, and as supported by the SMEs across all 3 worldviews, this siloed nature is currently an inhibiting force (Figure 2).

SMEs from all three worldviews (including [C, G, H, and L] from traditional security; [D, O, and R] from emerging security; and [E] from system analysis) also noted that understanding the underlying characteristics of security risk posed by new threats is necessary to better characterize both the known and unknown threat space. For example, UASs pose a challenge because they explicitly counter traditional two-dimensional thinking within security activities. In order to truly mitigate risks posed by UAS (or any other unmanned robotic system), the data suggests a need to consider three-dimensional vulnerability (i.e., above ground and below ground considerations). Moreover, some SMEs [O and R] noted that current threat categorizations (and associated security assessments) are strongly tailored towards a specific, defined threat. This approach often limits consideration of details about how specific underlying threat characteristics pose risk (e.g., how can a threat shut down an HCF site). In addition, one SME [H] mentioned how inadequate threat characterization could, hypothetically, result in the ability to modify adversary attributes relative to security system design and performance within security assessments.

Given the current threat-based approaches, the intent of security assessments tends toward being the only threat considered, as opposed to considering the larger system of possible threats and vulnerabilities of a given HCF site. Instead, SMEs [A, G, H, O, and R] recommended revisiting the original set of threats with techniques (such as modelling/simulation, performance testing, physical/cyber tabletop activities, and force on force exercises) to support better system analysis and threat assessment. An adaptive threat characterization process that captures emerging issues while supporting system design will support (or help) drive the systems toward a more ideal state (Figure 2). Likewise, accurate performance testing will help identify security performance gaps allowing for changes to address current and emerging threats. However, the current static and prescriptive nature of threat characterization and system evaluation is inhibiting the system from achieving its overall security goal (Figure 2).

An additional pattern within this theme relates to how SMEs from all three worldviews ([A, R, and FG2] from traditional security, [C, G, K, and I] from emerging security, and [N, P, and Q] from systems analysis) noted that the calculations associated with human activities in the security assessments require updates. One of the common equations involves calculating the probability of detection, a primary performance measure in security assessment methodologies, that describes the system's ability to sense, identify, and alert a malicious act [14]. Multiple SMEs (including [C and K]) noted that the calculations for the probability of detection "lacks rigor," with many values being assumed constant even when observations and data suggest that they should be treated as conditional values depending on the local context. For example,

SMEs [G, K, and FG2] noted that one of the largest assumptions in security and associated assessment activities are the capabilities of the security staff across differing locations. For example, the Central Alarm Station (CAS) operator's ability to correctly identify an issue when they are being inundated by false/nuisance alarms is not adequately incorporated into the security assessment calculations. In fact, the competence level of the CAS operators is often assumed to be between adequate and ideal, with simplistic suggestions offered for downgrading probability of detection of the operator by some nominal percentage when "poor performers" are present [15].

Such approaches do not accurately represent the impact that ineffective operational activities could have on site security. Studies like [38] have demonstrated, for example, the prevalence effect in human-led screening activities, whereby an individual is more likely to fail to detect a target with low prevalence (i.e., frequency) than a target with higher prevalence, especially when feedback about accuracy is not provided. Such limited understanding of human and organizational factors extends into inaccurate effectiveness evaluations of different interventions (e.g., leading to assumptions that two fences will cause twice the delay as a single fence [FG2] or pan/tilt/zoom cameras will be used as intended [FG2]) and credibility of emerging threats (e.g., when collusion is not considered in insider analysis [A and P]). SME [P] noted that collecting relevant data to better understand these dynamics requires significant effort and can be challenging because current examples are often informed by extreme cases, though one SME [A] noted that databases are being introduced to track and measure such data. In addition, SMEs [I and O] noted that organizational factors also need to be more effectively considered. For example, the requirements of the assessments themselves seem to incorporate customer biases and solution preferences [D, F, and O]. Another issue identified by SMEs ([D and I]) was the impact of the assessment outcome on site personnel job security. Resulting dynamics will likely look different if, for example, the security manager is fired for a failed assessment versus establishing a corrective action plan (i.e., non-punitive testing). These biases influence the actual implementation of the security assessment (Figure 2). Current assumptions and models (especially of human activities) are inhibiting actual security performance evaluation (Figure 2), leading to unidentified and uncorrected gaps and flaws, which can create a false sense of confidence.

Theme 3: Cultural Influences

The final common theme identified in the data relates to a wide range of non-technical and social factors on security operations and performance, such as institutional dynamics, formal and informal policies, and attitudinal influences on the state of security. Such considerations and related policy issues were identified by traditional security professionals while risk attitudes were highlighted more by emerging security and systems analysis professionals (Figure A2).

Policies were identified as a significant driver of both security assessment activities and the state of HCF security. For example, SME [M] noted an improvement in the state of nuclear security after President Obama signed the Convention on the Physical Protection of Nuclear Material into law, which advanced regulatory and legal considerations of security activities within the United States [39]. Generally, security-related policy was described as a "double edge sword" (SME [O]) with guidance being not as strong as it could be in some places or too rigid in others. Cybersecurity and human factors were two areas identified by SMEs (including [B] and [O]) that generally lacked in policy guidance. Policies are often prescriptive and limited to minimal requirements, and often may not accurately mirror the threat. Where policy is not prescriptive, compliance-driven versions are often employed. According to data from across worldviews, such processes negatively influence attitudes of security implementers and operators, resulting in an inhibiting force away from the ideal state of security (Figure 2). In contrast, all worldviews indicated that adaptive and performance-based policies support moving toward the ideal state of security.

HCF security attitudes were predominantly described as "risk-averse," which manifests in multiple ways. For example, SME [H] highlighted that understanding challenges to current security performance or emerging adversary capabilities in the United States follows a "seeing is believing" mentality. This approach generally discounts issues or concerns seen overseas, leading to security personnel "almost always fighting the last war" (SME [P]). Here, lack of

concern regarding current HCF security capabilities is considered to reinforce a status quo mentality that support incremental HCF security paradigm changes. This is in stark contrast to the need for changing inherent HCF security paradigms expressed by SMEs across worldviews, including SMEs [D and R] from traditional security; SMEs [G and H] from emerging security; and SMEs [E, F, and FG1] from systems analysis. Cultural influences also manifest "on the ground," as SMEs [C, I, and R] described how security analysts are often set in their ways and approaches, making it challenging for them to discuss cross-sector issues or observe unaddressed interdependencies, which connects back to issues of changing operational designs and contexts (Theme 1). These cultural influences (which are sometimes driven by sponsor and customer priorities [D, F, J, O, and Q]) serve to inhibit change towards an ideal security state (Figure 2).

Opportunities for Improvement

In reaction to the current siloed nature of security activities, SMEs from all three worldviews noted that security should be approached from a systems perspective (Figure A2). This includes proactive consideration of threats (SME [G]) that balances mitigation versus removal threats. The systems perspective is needed to ensure that vulnerable assets are being adequately protected regardless of the specific threat. SMEs (e.g., [F]) emphasized that security assessments should lead to actionable or intelligible information regarding current security performance insufficiencies. This requires a close alignment between the assessment technique(s) and observed operations so that subsequent decisions are contextualized and well-informed (SME [I]). Finally, SMEs noted that an ideal state of security also takes into account cognitive behaviours, through effective human-machine teaming (SME [M]) and instilling a sense of security and empowerment (SME [FG1]) amongst the team to "proactively engage" (SME [Q]) in being part of future security solutions.

Two opportunities identified in the SME data could help shape such a proactive transition from the current state toward a more ideal state: 1) knowledge management and 2) improved metrics. As identified in the SME data, multiple factors influence both security performance and the dynamics in which such systems operate (Figure 2), which suggests a need to better coordinate between them. Given that these factors can also interact, describing security performance as an emergent property may offer a better understanding of the larger security system itself. For example, SME [J] noted that ideal security requires information to be filtered in order to balance improved decision-maker effectiveness with sufficient operational redundancy to reduce overall performance dependency on individual components. Additionally, bridging the silos between different parts of the security system can be challenging due to different languages (and associated cultures) existing in different areas of security (SME [L and P]). By clarifying functional roles (e.g., infrastructure operations might focus on ensuring continuous power supply to a site while cyber operations focus on mitigating digital adversarial capabilities) and aligning overarching security performance objectives (e.g., ensuring the HCF achieves its critical mission by protecting against malicious actions), a systems approach could improve coordination with operational priorities and help reduce barriers to achieving the ideal state of security.

The data also suggests a need to better understand the roles individuals play in overall security performance, particularly when considering the increase in digital controls. In many ways, human-machine interactions attempt to leverage the respective strengths of each (e.g., machines have a superior long-term capability to execute rote, mundane tasks). However, to ensure that such investments continue to operate as intended under changing conditions presupposes a need to ensure the specific intent of "why" certain design or operational decisions were made are recorded and communicated over the lifetime of HCF security operations. Not doing so, according to SME [D], can negatively impact future attempts to improve technological upgrades and integration, potentially leading to unintended consequences. Put more pointedly,

> ""Historically, [it is] likely [that we] had rich conversations about the [security assessment] framework and associated caveats and assumptions…[while] the framework has been passed on, the continuous improvement process has not been retained." – SME [N]

During significant technological and methodological shifts, SME [K] noted that the value of revisiting guiding principles of security to ensure the underlying intent of related activities are not lost during transitions and evolutions.

Finally, SMEs noted that the current implementation of security assessments are strongly driven by the specific metrics that are used to assess outcomes. Informed by guidance from various stakeholders, per SME [A], current metrics primarily emphasize the timeliness of response with a focus on: 1) success rate, 2) access/proximity to target, 3) duration of engagement, and 4) casualty rate. However, SMEs from multiple worldviews (including [R and FG2] from traditional security, [G, H, and K] from emerging security, and [FG1] from systems analysis) asserted that these metrics do not align well with the overall security performance. Another shortcoming noted in the SME data includes the inadequate capture of near-miss or undisclosed security events, as noted by SME [FG1] where they "worry about the ones that are not reported." Instead, SMEs [M, P, and FG1] recommended that the specific metrics used for security assessments should also support deterrence activities as well as overall security performance (including consequences) (Table 3).

Table 3. Systems-Level Questions to Guide Metrics Development.

SME Insight	**Systems Theory Concept**	**Questions to Guide Metrics**
"… a systematic view is needed that looks beyond compliance with the regulations, but also considers emergency response, cyber vulnerabilities, as well as safety and security issues." [M]	Identify key interactions & interdependencies	• How can interactions between disparate aspects of security be measured?
"What does the full system do? What does it need to do it? How does it all link together?" [M]	Define overall system objective	• How can "effectiveness" in achieving the overall objective be measured?
"Performance measures need to be defined uniquely for the system ... Balancing 'risk' vs 'resources' can be a barrier." [C]	Identify trade-offs between key performance measures	• How can stakeholder biases be captured in consequence measures? • Can multi-objective decision analysis help characterize the security performance trade-off space?
"…ensure that consequences are looked at over time: temporal disconnects between threats and consequences are assessed dynamically." [E]	Account for impact of dynamics within the system	• How can relative preference for adversary action be measured? • How can temporal influence be adequately captured in design and analysis?
"Can figure out details in reverse – figure out what consequences are important, and then figure out what characteristics of the infrastructure could result in these consequences?" [E]	Describe emergent system properties from different logical perspectives	• How to prioritize consequences based on assume adversary success? • How to account for stakeholder biases in consequence prioritization?
"We need to consider changing the end state from just stopping the bad guys to include considering how they may be changing (what did they learn) and measure the overall system stability and flexibility." [R]	Account for naturally evolving relationship between system & its environment	• What system properties help describe observed dynamics in HCF security? • Can adversary intentionality (or learning) be described through system or environment boundary changes?
"Sensor algorithms need to move from rule-based approaches to empirical-based approaches that are informed by both the original data as well as the feature vectors capturing the rules from the former." [K]	Increase operational feedback	• How can security system "learning" be measured?

Specifically, SMEs emphasized that metrics should be guided by a larger understanding of security system, including both defensive and offensive perspectives. For example, one cyber resilience SME [C] described a generic process of developing four basic metric categories for conducting their analyses: physical, network, host, and intrusion detection systems [40] [41]. Within each of these categories, performance metrics are tailored to a specific case (e.g., time to first violation may be more important in some cases, whereas total number of violations may be important in others). Resilience SMEs [E and F] noted the importance of being mindful of the spatiotemporal aspects of performance metrics, such as considering both the number and duration of resources required to achieve necessary security performance. Security SMEs [A, G, H, O, and R] noted that such diverse strategies as simulations and modelling, hands on testing, tabletop, and force-on-force exercises could be leveraged to inform metrics. There was an undercurrent in the data suggesting that future security metrics should consider both quantitative and qualitative approaches to effectively assess security performance. Lastly, the SME data identified the importance of obtaining stakeholder support for incorporating new security metrics for improving and enhancing security assessment activities. In Table 3, key concepts identified in the SME data were aligned with systems theory-related concepts and translated into questions to guide future metric development inclusive of key empirically-identified attributes.

Discussion

The themes from the SME data highlight many of the challenges observed in current HCF security approaches as well as identified opportunities for overcoming them. Namely, SME data identified the changing operational designs and contexts are a reality that influence both the current state of a security as well as associated assessment activities. However, methodological shortcomings (compounded by cultural influences) impact the utility and accuracy of current assessments. The worldview perspective of the data analysis provided a useful framing to evaluate the implications of commonalities between traditionally disparate perspectives of HCF security. For example, issues of maintenance, siloed system activities, and human factors were recognized by SMEs from all three worldviews while issues of location and policy were predominantly identified by practitioners within the traditional security worldview (Figure A2). Summarizing insights from SMEs into an FFD helps identify conflicting factors as well as opportunities to address them.

Although only Sandia personnel were consulted for this analysis, the need for a systems approach that considers cultural, managerial, and educational factors has been identified in related security fields, such as intelligence analysis [42] [43]. Furthermore, interviewed SMEs reflect diverse roles in HCF security that reflect Sandia's cornerstone role in the development and implementation of the current set of security assessment approaches (e.g., [15]). The extent of consistency between the three worldviews indicates a level of validation for these empirical themes. One may expect that the emerging security worldview would be particularly sensitive to the methodological shortcomings and the systems analysis worldview would be more likely to discuss elements of the cultural influences theme. However, the SME data indicates that all three worldviews acknowledged each theme, albeit with varying frequencies (Figure 1; Figure A2). This observed consistency between worldviews not only supports the importance of these themes for better understanding challenges to current HCF security capabilities, but also offers implications for how to transition toward ideal future HCF security states.

This research supports arguments for new security assessment approaches to keep up with the recent advances in adversary capabilities, as well as changes in operational environments and non-traditional influencing dynamics. Specifically, the adoption of a systems approach was iterated by almost all SMEs (17/20) across all three worldviews. A systems approach that recognizes the dynamic interaction between components could help reduce the siloed behaviour currently observed in security activities through improved knowledge management and metrics used for assessment. Specifically, using a systems approach for coordination within security systems and increased understanding of functional intent of security performance in conjunction with improved metrics for security performance can serve to transition towards an ideal state of security. The metrics-guiding questions (Table 3) will help ensure underlying system dynamics are sufficiently being addressed across different threats.

A recognition of gaps in current security assessment activities indicates that past hesitation to accept new approaches to HCF security may be dissipating. SME insights underscore a critical need to re-evaluate core assumptions of the state of HCF security, including “soft” influences and associated dynamics interactions. These “soft” influences range from due consideration of human performance capabilities in security assessments and risk attitudes to improvement understanding of functional roles and metrics development using a systems-based approach. Ultimately, using a systems paradigm for HCF security will provide a strong foundation for improving gaps in current operations and assessments that impact HCF security performance efficiency and effectiveness against real-world complexities, innovative adversaries, and disruptive technologies.

One effort to address these gaps conceptualizes HCF security as a multi-layered network (MLN), where nodes represent key assets (e.g., cameras and guards) and edges representing different types of connectivity between nodes (e.g., data transmission) [44]. Preliminary results from such an approach seem to directly address the major themes emerging from the SME data emphasized by SMEs across all three worldviews, namely the explicitly accounting for human actors and improved metrics [44] [45]. Moreover, the HCF security performance metric development approach summarized in Table 3 also seems to align with the suite of MLN performance measures (such as multilink community detection, versatility, and multilayer communicability [39]) that may better capture the complex challenges facing HCF security. The MLN model approach could also be integrated into ongoing testing strategies (e.g., tabletop and redteaming exercises) to support the evaluation of both qualitative and quantitative performance evaluations of HCFs [44]. Such innovative approaches that leverage the analytical constructs and performance measures better will be needed to ensure that security assessments continue to reduce risks in HCF security.

Conclusion

This study highlighted common themes (among SMEs with diverse worldviews) associated with current security assessments: 1) changing operational designs and contexts, 2) methodological shortcomings, and 3) cultural influences. While the latter is heavily influenced by external factors, security assessments could be modified to better address concerns raised in the first two themes. For example, better accounting for how sensors operate in certain conditions and factors impacting human conditions (i.e., operators’ abilities to successfully identify issues among false alarms) would increase the mathematical rigor, and thus, the accuracy of security assessments. Such capabilities are enabled by use of new modelling and simulation techniques (such as multi-layered networks) to better capture the assumptions and dependencies of current systems (i.e., knowledge management) and enable more effective assessments of emerging behaviours through improved metrics. These methodological advancements in conjunction with ongoing investments in training, monitoring, and maintenance will ensure that security assessments will continue to support HCFs so that they are secure (through changing operational contexts) against emerging threats.

Acknowledgements

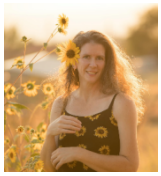
The authors would like to thank Jami Stverak for assistance with data collection and Elizabeth Fleming for providing feedback on an earlier version of the manuscript. This work was supported by the Laboratory Directed Research and Development program at Sandia National Laboratories, a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. The views expressed in the article do not necessarily represent the views of the U.S. Department of Energy or the United States Government. Additional information about the data presented in this paper can be procured from contacting the corresponding author.

Keywords

high consequence facilities, security assessments, complex systems, subject matter experts, worldviews, multi-layered network

Author Biographies

Thushara Gunda is a Principal Member of Technical Staff at Sandia National Laboratories. She holds bachelor's degrees in environmental science and environmental policy from the University of Virginia, and a PhD in environmental engineering from Vanderbilt University. She implements data science for interdisciplinary projects across energy, water, and security domains.



Sue Caskey is a Principal Member of the Technical Staff at Sandia National Laboratories. Sue has over 20 years' experience in Global Security and Non-Proliferation and worked on CBRN security issues in more than 30 countries. She has bachelor's degrees in biology and computer science from the University of New Mexico and a master's in engineering focusing on systems engineering from Old Dominion University.

Adam D. Williams is a Principal R&D Systems Engineer in the Center for Global Security and Cooperation at Sandia National Laboratories. He has a bachelor's degree in mechanical engineering, a master's degree in international affairs from Texas A&M University, and a Ph.D. in human-systems engineering from the Massachusetts Institute of Technology. At Sandia, he develops and applies systems-theoretic solutions to various national and nuclear security challenges.

Gabriel C. Birch is a Principal R&D Optical Engineer in the Weapons and Force Protection Center at Sandia National Laboratories. He has a bachelor's degree in optical engineering as well as a master's and Ph.D. in optical sciences from the University of Arizona. At Sandia, he develops novel solutions to physical problems for high consequence facilities.

References

[1] Cyber Infrastructure Security Agency, U.S. Department of Homeland Security, “Critical Infrastructure Sectors,” 4 March 2020. [Online]. Available: https://www.cisa.gov/critical-infrastructure-sectors.

[2] C. Alcaraz and S. Zeadally, “Critical infrastructure protection: Requirements and challenges for the 21st century,” *International Journal of Critical Infrastructure Protection,* vol. 8, pp. 53-66, 2015.

[3] B. Hubbard, P. Karasz and S. Reed, “Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran,” The New York Times, 19 September 2013. [Online]. Available: https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html. [Accessed 4 March 2020].

[4] A. Campbell and V. Singh, “Lessons from the cyberattack on India's largest nuclear power plant,” Bulletin of the Atomic Scientists, 14 November 2019. [Online]. Available: https://thebulletin.org/2019/11/lessons-from-the-cyberattack-on-indias-largest-nuclear-power-plant/. [Accessed 4 March 2020].

[5] Cybersecurity Insider, “Insider Threat 2018 Report,” 2019. [Online]. Available: https://www.veriato.com/resources/whitepapers/insider-threat-report-2018. [Accessed 30 May 2020].

[6] M. Bunn and K. M. Glynn, “Preventing Insider Theft: Lessons from the Casino and Pharmaceutical Industries,” *Journal of Nuclear Materials Management,* vol. 41, no. 3, 2013.

[7] Nuclear Engineering International, “Russian floating nuclear plant supplies 10Gwh of electricity ro Chuktoka,” Nuclear Engineering International Magazine, 2020. [Online]. Available: https://www.neimagazine.com/news/newsrussian-floating-nuclear-plant-supplies-10gwh-of-electricity-to-chukotka-7741808. [Accessed 10 June 2020].

[8] International Atomic Energy Agency, “Security aspects of nuclear facilities,” [Online]. Available: https://www.iaea.org/topics/security-aspects. [Accessed 30 May 2020].

[9] R. M. Salerno and J. Gaudioso, Eds., Laboratory biorisk management: biosafety and biosecurity, CRC Press, 2015.

[10] A. Nelson and M. Mulcahy, “Chemical security handbook: Security Risk Assessment for Laboratories,” Albuquerque, NM, USA, 2020.

[11] International Atomic Energy Agency, “Nuclear Security Assessment Methodologies for Regulated Facilities: Final Report of a Coordinated Research Project,” 2019.

[12] G. Wyss, J. Clem, J. Darby, K. Dunphy-Guzman, J. Hinton and K. Mitchiner, “Risk-based cost-benefit analysis for security assessment problems,” in *44th Annual 2010 IEEE International Carnahan Conference on Security Technology*, IEEE, 2010, pp. 286-295.

[13] A. D. Williams, G. C. Birch, T. Gunda, S. A. Caskey, T. Adams, J. Wingo and J. Stverak, “Empirical Insights for a Multi-Layered Network Complex Systems Model for Engineering Nuclear Security Systems,” in *61st Annual Meeting of the Institute of Nuclear Materials Management*, 2020.

[14] W. J. Desmond, N. R. Zack and J. W. Tape, “The First Fifty Years: A Review of the Department of Energy Domestic Safeguards and Security Program,” *Journal of Nuclear Materials Management,* vol. 26, no. 2, 1998.

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

[16] B. Zou, “Evaluation of vulnerable path: Using heuristic path-finding algorithm in physical protection system of nuclear power plant,” *International Journal of Critical Infrastructure Protection,* vol. 23, pp. 90-99, 2018.

[17] K. Kampova, T. Lovecek and D. Rehak, “Quantitative approach to physical protection systems assessment of critical infrastructure elements: Use case in the Slovak Republic,” *Journal of Critical Infrastructure Protection,* vol. 30, 2020.

[18] Science Applications International Corporation (SAIC), “A Guide to Highway Vulnerability Assessments for Critical Asset Identification and Protection,” Vienna: Transportation Policy and Analysis Center, 2002.

[19] A. A. Sadiq, “Chemical Sector Security: Risks, Vulnerabilities, and Chemical Industry Representatives' Perspectives on CFATS,” *Risk, Hazards & Crisis in Public Policy,* vol. 4, no. 3, pp. 164-178, 2013.

[20] F. A. Duran, G. D. Wyss, S. E. Jordan and B. B. Cipiti, Risk-Informed Methodology for Enterprise Security: Method and Applications for Nuclear Facilities, Albuquerque, NM, USA: Sandia National Laboratories, 2013.

[21] L. Cox, "What's Wrong with Risk Matrices?," *Risk Analysis,* vol. 28, no. 2, pp. 497-512, 2008.

[22] E. Zio, "Challenges in the vulnerability and risk analysis of critical infrastructures," *Reliability Engineering System Safety,* pp. 137-150, 2016.

[23] A. Williams, "Beyond Gates, Guards, & Guns: The Systems-Theoretic Framework for Nuclear Security," Massachusetts Instistute of Technology, Dissertation, Cambridge, MA, 2018.

[24] J. R. Stainback IV and W. J. Toth, "Human-Complex System Interactions and Complacency within High Consequence Facilities," in *Proceedings of the Annual Meeting of the Institute for Nuclear Materials Management*, 2013.

[25] O. L. De Weck, D. Roos and C. L. Magee, Engineering systems: Meeting human needs in a complex technological world, MIT Press, 2011.

[26] A. Lauge, J. Hernantes and J. M. Sarrigei, "Critical infrastructure dependencies: A holistic, dynamic and quantitative approach," *International Journal of Critical Infrastructure Protection,* vol. 8, pp. 16-23, 2015.

[27] K. M. Adams, "Perspective 1 of the SoSE methodology: framing the system under study," *Int. J. System of Systems Engineering,* vol. 2, no. 2/3, pp. 163-192, 2011.

[28] R. D. Weiss, Learning from Strangers: The Art and Method of Qualitative Interview Studies, New York: The Free Press, 1995.

[29] M. B. Line, I. A. Tøndel and M. G. Jaatun, "Current practices and challenges in industrial control organizations regarding information security incident management – Does size matter? Information security incident management in large and small industrial control organizations," *International Journal of Critical Infrastructure Protection,* vol. 12, pp. 2-26, 2016.

[30] L. Petersen, "Resilience for Whom? The general public's tolerance levels as CI resilience criteria," *International Journal of Critical Infrastructure Protection,* vol. 28, 2020.

[31] F. Landegren, M. Höst and P. Möller, "Simulation based assessment of resilience of two large-scale socio-technical IT networks," *International Journal of Critical Infrastructure Protection,* vol. 23, pp. 112-125, 2018.

[32] J. Horton, R. Macve and G. Struyven, "Qualitative Research: Experiences in Using Semi-Structured Interviews," in *The Real Life Guide to Accounting Research*, C. Humphrey and B. Lee, Eds., Elsevier, 2004, pp. 339-357.

[33] T. O. Nyumba, K. Wilson, C. J. Derrick and N. Mukherjee, "The use of focus group discussion methodology: Insights from two decades of application in conservation," *Methods in Ecology and Evolution,* vol. 9, no. 1, pp. 20-32, 2018.

[34] M. Hibberts, R. Burke Johnson and K. Hudson, "Common Survey Sampling Techniques," in *Handbook of Survey Methodology for the Social Sciences*, L. Gideon, Ed., New York, NY, USA, Springer New York, 2012, pp. 53-74.

[35] A. Strauss and J. M. Corbin, Basics of qualitative research: Grounded theory procedures and techniques, Newbury Park, CA, USA: Sage Publications, Inc., 1990.

[36] R. T. Lange, "Inter-rater Reliability," in *Encyclopedia of Clinical Neuropsychology*, J. S. Kreutzer, J. DeLuca and B. Caplan, Eds., New York, NY, USA, Springer New York, 2011, p. 1348.

[37] H. Sillitto, R. Griego, E. Arnold, D. Dori, J. Martin, D. McKinney, P. Godfrey, D. Krob and S. Jackson, "What do we mean by "system"? – System Beliefs and Worldviews in the INCOSE Community," *INCOSE International Symposium,* vol. 28, no. 1, pp. 1190-1206, 2018.

[38] J. Wolfe, D. Rubinstein and T. Horowitz, "Prevalence effects on newly trained airport checkpoint screeners: Trained observers miss rare targets, too," *Journal of Vision,* vol. 13, no. 3, 2013.

[39] International Atomic Energy Agency, "United States Ratifies Key Nuclear Security Amendment," 2015. [Online]. Available: https://www.iaea.org/newscenter/news/united-states-ratifies-key-nuclear-security-amendment. [Accessed 25 June 2020].

[40] S. Hossain-Mckenzie, C. Lai, A. . Chavez and E. Vugrin, "Performance-Based Cyber Resilience Metrics: An Applied Demonstration Toward Moving Target Defense," in *IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society*, 2018.

[41] N. Jacobs, S. Hossain-McKenzie and E. Vugrin, "Measurement and Analysis of Cyber Resilience for Control Systems: An Illustrative Example," in *2018 Resilience Week (RWS)*, 2018.

[42] J. Kerbel, "Studies in Intelligence," *Journal of the American Intelligence Professional,* vol. 48, no. 3, 2004.

[43] S. M. Beebe and G. S. Beebe, "Understanding the Non-Linear Event: A Framework for Complex Systems Analysis," *International Journal of Intelligence and CounterIntelligence,* vol. 25, no. 3, pp. 508-528, 2012.

[44] A. D. Williams, G. C. Birch, S. Caskey, T. Gunda, J. Wingo and T. Adams, "A Complex Systems Approach to Develop a Multilayer Network Model for High Consequence Facility Security," in *International Conference on Complex Systems*, 2020.

[45] G. Binaconi, Multilayer Networks: Structure and Function, Oxford: Oxford University Press, 2018.

Appendix

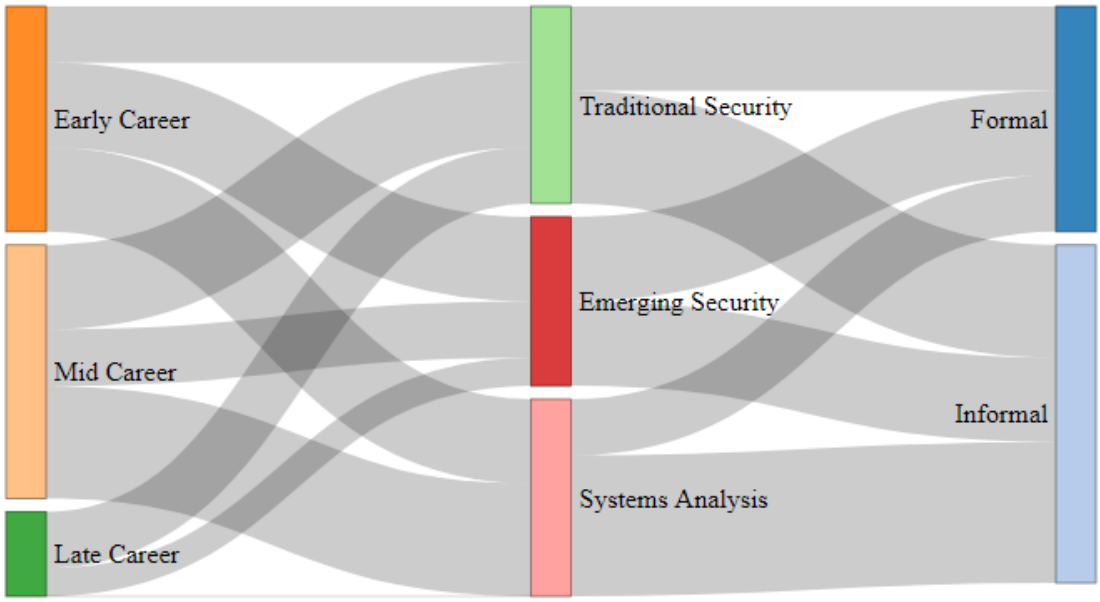


Figure A1. Demographic Profile of SMEs Worldviews. The width of the bands is linearly proportional to the number of SMEs within a given Worldview (center of the diagram) that have formal or informal training (right side of diagram) and their career stages (left side of diagram). Early career refers to 1-9 years of experience, Mid-career: 10-19 years, and Late career: 20+ years.

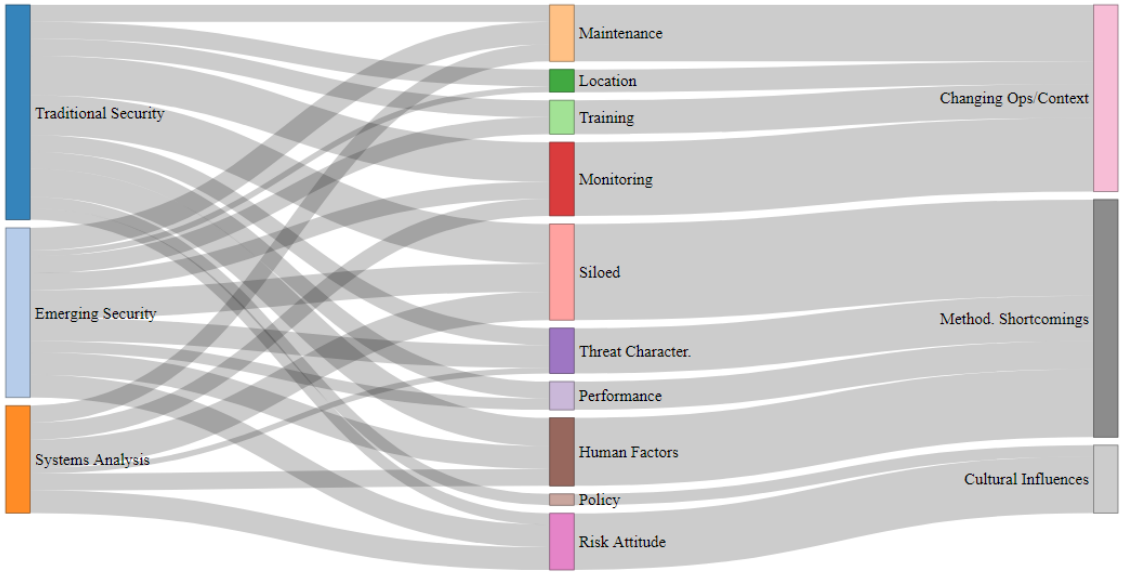


Figure A2. Sankey Diagram of World Views and Subthemes of Common Themes. The width of the bands is linearly proportional to the number of quotes/anecdotes shared by a given worldview (left side of the diagram) regarding the subtheme (center of the diagram) of a given common theme (right side of the diagram).

Figure A3. Emerging threats highlighted by SMEs. The size of the words reflects the relative frequency of the term; larger words (e.g., UAS) were mentioned more frequently by SMEs than smaller words (e.g., helicopters).