SAND2022-8244C

LESSONS LEARNED FROM EXPLORING SAFETY, SECURITY, AND SAFEGUARDS INTERFACES IN ADVANCED AND SMALL MODULAR REACTOR TECHNOLOGIES

A.D. WILLIAMS[1], B.B. CIPITI[1], J.J. BLAND[1], D.M. OSBORN[1], A.S. EVANS[1]

[1]Sandia National Laboratories, Albuquerque/New Mexico, United States of America

Abstract

Evolutionary and innovative reactor technologies are moving toward smaller and advanced designs that will impact the ability of nuclear installations to achieve desired levels of safety, security, and safeguards (3S). Yet, such technologies also present new opportunities to address 3S interfaces. For example, as installation operators seek reduced physical protection footprints, they may apply knowledge of safety systems to mitigate potential sabotage scenarios and align material monitoring for international safeguards with accounting for security. Similarly, the anticipated increase in digitization and automation in nuclear installations to support these reactor technologies enhances the importance of addressing cyber interfaces to ensure adequate 3S operations. In response, Sandia National Laboratories (Sandia) has supported a range of research projects and design-related engagements to better understand different 3S interfaces for advanced reactor technologies and facilities. The paper will review a set of Sandia-developed examples demonstrating opportunities related to 3S interfaces. Supported by both research-based analysis and practical experience, risk reduction strategies for such reactors and installations are enhanced when accounting for interfaces in both 3S operations and uncertainty. The conclusions, insights, and implications from these examples help frame approaches to better address 3S interfaces in designing, deploying, licensing, operating, and decommissioning evolutionary and innovative reactors.

1. INTRODUCTION

Current levels of interest in advanced and small modular reactors (A/SMR) are driving additional conversations regarding the impacts of integrated safety, security and safeguards interfaces in responsible operations. Both international (the World Institute for Nuclear Security) and national (the U.S. National Academy of Sciences) have advocated for an "all-hazards approach [1]" and "a 'total systems approach' to characterize the interactions and dependencies [2]" for risk reduction in peaceful nuclear operations. Former Deputy Director-General for Safeguards at the International Atomic Energy Agency Olli Heinonen described it well:

> *Safeguards, security, and safety* are commonly seen as *separate areas* in nuclear governance. While there are technical and legal reasons to justify this, they also *co-exist and are mutually reinforcing*. Each has a *synergetic effect on the other*, and authorities should carve out avenues for collaboration to contribute to the effectiveness of the nuclear order. For instance, *near real-time nuclear material accountancy and monitoring systems* provide valuable information about the location and status of nuclear material. This in turn is useful for *nuclear security* measures. Similarly, such information enhances *nuclear safety* by contributing as input to critical controls and locations of nuclear materials. [3] (Emphasis added)

The legacy of traditional nuclear power facilities (and fuel cycle activities)—guided by technical, regulatory and research-based drivers—is to separate safety, security and safeguards design and operations. Yet, the move toward smaller and more operationally agile A/SMRs indicates a need to re-evaluate traditional (and often isolated) safety, security and safeguards approaches. In particular, today's context supports renewed resources for exploring opportunities for (and potential benefits of) better understanding safety, security and safeguards (the so-called "3S") interfaces. For example, opportunities may exist to apply safety systems to mitigate potential sabotage scenarios or to align material monitoring for safeguards with accounting for security. Capturing 3S interfaces will only grow in importance given the anticipated increased digitization expected in A/SMR-related facilities.

Several A/SMR trends may result in more overlap between and among safety, safeguards, and security (see Fig. 1), including (but not limited to):

— Smaller operational footprints
— Increased deployment flexibility
— Novel fuel types (including physical attributes)
— New fuel flows & handling systems
— Increased automation in operations
— Smaller onsite staffing

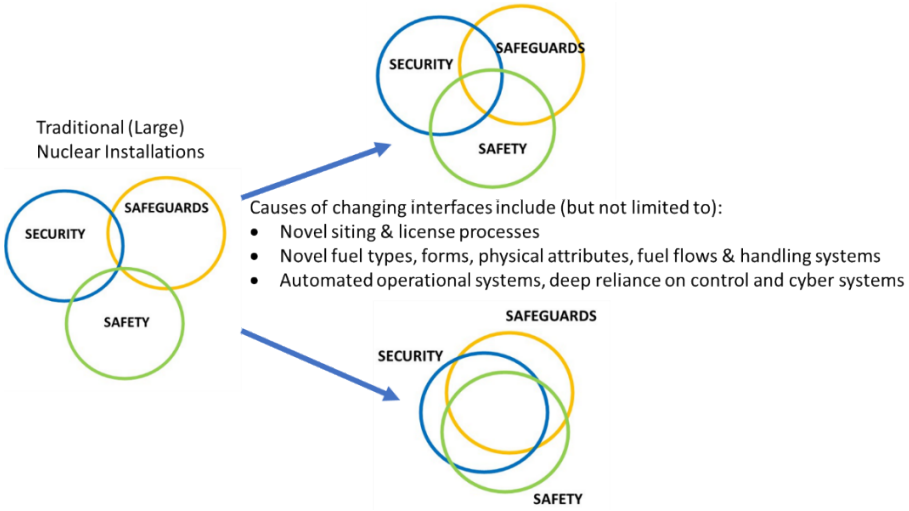

FIG. 1. Conceptual illustration of varying safety, security and safeguards (3S) interfaces across different reactor designs.

This is potentially a tectonic shift in nuclear power operations as these facilities will likely need to move beyond lessons learned from conducting safety, security, and (international) safeguards at traditional nuclear power facilities. Additional benefits from addressing 3S interfaces could aid in navigating and aligning with new regulatory options as specific A/SMR technologies progress in their licensing processes. Developing and implementing approaches to better characterize 3S interfaces seems well poised to better address the challenges facing—and enhance the potential benefits of—A/SMRs.

Through a combination of United States Government-supported research projects—including from several U.S. Department of Energy and National Nuclear Security Administration programs—and design engagements across a range of U.S. A/SMR vendors, Sandia National Laboratories (Sandia) has explored various approaches to better understand the 3S interfaces for advanced reactor technologies and facilities. The rest of this paper summarizes a representative set of lessons learned on how accounting for 3S interfaces can improve risk reduction strategies for A/SMRs. The conclusions, insights, and implications from these examples help frame approaches to better address 3S interfaces in designing, deploying, licensing, operating, and decommissioning evolutionary and innovative reactors.

2. SAFETY-SECURTY-SAFEGUARDS EXAMPLES IN ADVANCED & SMALL MODULAR REACTORS

Consider the following examples summarizing three cases of exploring 3S interfaces for A/SMRs. These examples include the impact of 3S interfaces on technical, regulatory and deployment aspects of A/SMRs. Synthesized from several Sandia research projects, these examples help clarify the need for better addressing 3S interfaces, as well as the potential for improving “by-design” approaches for A/SMR for more efficient risk reduction.

2.1. Security-Safety Interfaces in SMRs

A key challenge small reactors face is maintaining adequate physical protection with reduced response force staffing. As the power output of advanced reactors decreases, the budget for physical protection (ideally) should be reduced proportionally to maintain economic attractiveness for such power plant designs. Yet, this is juxtaposed against the likelihood that a particular country's design basis threat (DBT) will not change—driving a need for new approaches to address the contrasting need to reduce physical security costs while also mitigating similar levels of threat. For example, consider the staffing logistics necessary to adequately cover normal (e.g., different daily shifts) and off-normal (e.g., weekends, holidays, etc) operations. Security costs to mitigate a country's DBT can easily burden operations if not addressed—and, ideally, optimized—ahead of time. (NOTE: These challenges become even more acute for microreactor designs.) In response, Sandia is evaluating different options for designing and deploying physical protection solutions that balance these two constraints, including:

- enhancing delay to support increased reliance on off-site response [4]
- increasing efficiency of on-site response designs and tactics
- implementing advanced security technologies—such as remote operation weapons systems (ROWS), like the example in [5]—to compensate for reduced on-site response personnel

The effectiveness of these new approaches, however, can be enhanced with safety-informed engineering. For example, if A/SMR designers better understand expected consequences of sabotage, then potential targets can be more comprehensively (and efficiently) identified. Consider the following scenario as an exemplar for the benefit of an integrated approach that addresses security/safety interfaces. In any given A/SMR, the most critical targets will likely be the reactor itself and any spent fuel in on-facility storage. In this case, it is more efficient to keep these potential targets physically co-located to minimize the number of geographical areas within a facility that need higher levels of security elements. With fewer physical areas/assets to protect, advanced security system designs could include limiting access points that can be designed to provide high levels of protection and/or deploying ROWS—both of which help compensate for minimal on-site staffing. This security design option is based on a denial strategy the focuses on preventing adversary access to critical areas or assets with elements mitigating both outsider and insider threats.

Yet, while this security design approaches ensures vital areas and assets are protected, there may still be potential for an adversary to target other, "less-critical" facility components to initiate more damage to the A/SMR facility in more indirect ways. For example, damage to any decay heat removal systems could put the reactor into a hazardous state that may not be fully realized for many hours or even days. To mitigate loss of decay heat removal, most A/SMR designs rely on smaller source terms and advanced safety systems to keep the reactor in a safe shutdown for long periods of time—ideally until cooling can be restored. This suggests two security/safety interfaces for A/SMRSs. First, there may be a need for additional protection of "less-critical" facility components to mitigate their use as indirect sabotage targets. Second, decay heat removal systems (as well as recovery procedures) can play a role in delaying potential consequences of adversary sabotage. Such systems and procedures offer off-site security personnel substantial time to respond to the threat (e.g., getting off-site response to an A/SMR within an hour is challenging, but within 8 hours is much more realistic) and, if necessary, assist in recovering normal A/SMR operations. Though a simple example, an understanding of how decay heat removal systems (and recovery procedures) impact possible sabotage scenarios highlights the benefit of integrated design approaches capable of addressing safety-security interfaces for A/SMRs.

2.2. 3S Implications from New Nuclear Fuel Forms

Successful deployment of A/SMRs will, at least in part, be driven by revisiting the role of nuclear fuel form in safety, security and (international) safeguards design decisions. For example, light water reactor designs that use solid fuel assemblies face fewer (international) safeguards challenges given the straightforward nature of item material accounting-based solutions for such assemblies. Yet, the efficacy of item accounting-based solutions for nuclear materials is hampered by several of the more popular "advanced" reactor designs—including pebble bed and molten salt designs. Such designs are anticipated to have a greater reliance on bulk accounting-based approaches because the nuclear material is in pebble or liquid fuel form. In contrast to item accounting, bulk

nuclear material accounting approaches face increased challenges due to more complex—and uncertain—measurement capabilities. Such complications for bulk measurements may require A/SMRs to more heavily rely on containment and surveillance solutions to meet (international) safeguards obligations. Similar trends can also be observed in security, as there may be a need for advanced nuclear material accounting techniques, or novel solutions, to help mitigate the insider threat. As such, an integrated 3S approach can help capture the implications of new nuclear fuel forms and inform more effective security and (international) safeguards designs for advanced reactor facilities.

Consider pebble bed reactors, which are unique in that each individual pebble contains minute amounts of fissionable material. From a safety perspective, operations personnel need to measure the burnup of every pebble on discharge to determine performance efficiency and decide whether to return that pebble to the core or discharge it to a spent pebble storage canister. An individual pebble has similar importance from a security perspective, as the loss of even one spent pebble could represent the possibility for a radioactive dispersal device. Yet, from a safeguards perspective, accounting could occur on a per canister basis. If a canister contains the equivalent of a significant quantity, hypothetically 2000 pebbles, then the loss of an individual pebble would be of minimal safeguards concern. Looking at nuclear fuel in the form of individual pebbles illustrates several competing factors to be addressed to account for operational/safety, safeguards, and security performance requirements. An effective pebble handing system should include an integrated design including each of these perspectives [6].

In comparison, consider molten salt reactors (MSRs), which differentiate themselves in terms of having nuclear fuel in liquid form. From a safeguards perspective, MSRs might be challenging as preliminary research has shown that the overall measurement error can be higher than a goal quantity of fissionable material due to the challenges of bulk measurements [7]. To compensate, MSRs will likely need to rely more on additional measures like—including, but not limited to containment and surveillance—to meet international safeguards obligations. Liquid-based nuclear fuels also pose interesting security challenges advanced reactor facilities, including nuclear material accounting to mitigate insider threats. The technical and procedural measurement solutions selected for process monitoring (to ensure safe operation of the reactor) may also be used to support actinide accounting (safeguards) and/or asset measurement/tracking (security). Similar to pebble bed reactors, design decisions for liquid-based A/SMRs that include an integrated 3S perspective can enhance facility operations and make plant monitoring systems more efficient and cost-effective.

2.3. Impacts on Risk Management in A/SMRs

Whether from new fuel forms, novel reactor (and subsystem) characteristics or new operational procedures, A/SMRs will introduce new dynamics to traditional "risk" associated with producing civilian nuclear power. Design decisions across safety, security and (international) safeguards will both enhance and constrain the impact of these dynamics on traditional perspectives of risk management for A/SMRs. Consider, for example, the need to recognize and prioritize assets and spaces of particular risk. In response, A/SMRs may benefit from revisiting traditional approaches for combining probabilistic safety assessments (PSA) and vital area identification (VAI) into a comprehensive review of both safety and security risk. Briefly, this approach translates a component-based fault tree model of nuclear facilities (used to calculate safety risk) into a geographic area-based fault tree (to support security analysis). (See [8] for a more detailed explanation.)

Consider, for example, the established process for VAI [8] was developed for the existing fleet of light water reactors. While having demonstrated benefits from exploring the safety/security interface for traditional nuclear facilities, some of the underlying analytical assumptions may be in appropriate for A/SMR designs. At a conceptual level, the process of screening out very low probability initiating events for safety accidents in the PSA fault tree indicates that failure modes (and mechanisms) that *could be* intentionally initiated are excluded. While the depth of operating experience has mitigated this concern for light water reactors, related risks for A/SMRs cannot be mitigated in a similar manner. At a design level, the traditional VAI process as developed assuming an operating nuclear facility with a completed PSA, which again does not apply to A/SMRs. The benefits of this VAI approach could be expanded (and experienced earlier) if A/SMR design firms had a VAI framework to implement early (and regularly) in the design process. This could result in mitigating risk by using security concerns to inform safety designs and for safety decisions to influence security designs—an integrated approach that can support the economic viability of A/SMRs.

At an analytical level, the current VAI approach also struggles with accounting for passive (or inherent) safety systems. As a key tenant for nuclear newcomers and a major selling point for many proposed A/SMRs designs, passive safety systems are facility mitigations that do not rely on actions of the operator or control/electrical system feedback to bring the reactor into a safe shutdown state. Since passive safety systems do not have moving parts that can "fail," they would not be included in a PSA. Yet, systems that are designed to support a safe shutdown in the event of an *accident* may not mitigate events that are initiated by a malicious event. From this perspective, passive safety does not equate to passive security. Therefore, future facility designs can be enhanced by a VAI process more inclusive of events that fall outside of the standard PSA techniques to identify security risks related to A/SMRs.

Considering the increased complexity (and novelty) of A/SMR attributes—including but not limited to control systems, fuel flows, and physical design features—there is a need to explore safety/security (and international safeguards) interfaces to better identify, categorize and prioritize risk in these designs. Opportunities exist to improve the use of PSA and VAI to enable designers, security and safety professionals to simultaneously evaluate safety and security risks in a more effective, cross organizational manner. If current approaches to PSA and VAI offer efficiencies and enhancements, then efforts to extend these benefits (starting with the suggestions in this section) should be explored to better mitigate 3S-related risks in support of A/SMR deployment.

3. AN APPROACH TO 3S RISK REDUCTION

Since 2015, Sandia has developed analytic capabilities to better identify and characterize 3S interfaces—including technical evaluations to anticipate, assess, and address nuclear risks using advanced systems, technologies, expertise, and situational awareness tools. The focal point of these 3S analytic efforts is to identify—and ideally influence—nuclear facility design performance parameters to improve operational efficiencies [9,10]. Conclusions from this work have helped reframe 3S interface discussions from novel concept to engineering design processes aimed at reducing safety, security and safeguards-related risks.

Reframing the understanding of 3S interfaces begins with invoking key systems theory principles and complex systems engineering concepts. While systems theory is founded on the Aristotelian adage that "the whole is greater than the sum of its parts," three key principles are useful for explaining related phenomena. For example, consider the phenomena by which some systems behaviors at a given level of complexity are irreducible to (and thus, inexplicable by) the behavior or design of its component parts. This key first principle—emergence—goes beyond component-based explanations to capture how interactions among components within a system (or with environmental influences) drive system-level (or observed) behaviors. The second key principle—hierarchy—uses functional descriptions of system operations to identify and evaluate levels of system complexity that provides a scaffold for better characterizing interactions the result in emergent system behaviors. The third key principle—interdependence—incorporates the concept of feedback to describe how actions (or outcomes) in one component impact downstream actions (or outcomes), whether in the same component or another.

Taken together, these principles help guide ongoing Sandia research to better characterize multidomain interdependencies observed between long-established nuclear safety practices, internationally-mandated nuclear safeguards processes, and socio-technical nuclear security systems. Invoking these principles yields a complex systems engineering approach to account for observed behaviors emerging from safety-safeguards-security interactions in nuclear facilities. Moreover, such a complex systems engineering approach introduce the ability to successfully design and responsibly operate increasingly novel A/SMR facilities in increasingly complex operational environments. The ongoing 3S research at Sandia has demonstrated that better capturing these interactions includes characterizing:

- *Interdependencies*: impacts on operational risks shared across components
- *Conflicts*: oppositional forces between components that increase operational risks
- *Gaps*: missing (or necessary) relationships between components that increase operational risks
- *Leverage points*: naturally existing redundancies or compensatory effects that can potentially mitigate operational risks

From the 3S perspective, these four categories of interactions offer enhanced clarity for anticipated A/SMR behaviors. Despite the advertised benefits of A/SMRs, many of those benefits will manifest from better

understanding interdependent relationships between safety, security and safeguards within these facilities. Similarly, successful A/SMR deployment would also seemingly benefit from better characterizing how objectives from one "S" may negatively overlap with expected behaviors of another "S" (e.g., conflicts) and better identifying expected individual "S" operations whose absence negatively impacts component or system level behaviors (e.g., gaps). Conversely, the advertised benefits of A/SMRs can manifest by reinforcing expected individual "S" operations that positively overlap with expected behaviors from a different "S" to serve as potential "force multipliers" between safety, safeguards, and security.

TABLE 1. SUMMARY OF SYSTEMS ENGINEERING DESIGN GOALS IN SANDIA'S COMPLEX SYSTEMS ENGINEERING APPROACH TO NUCLEAR SAFETY, SECURITY, AND SAFEGUARDS.

3S Interaction	Systems Engineering Design Goal
Interdependency	Identify & reconcile (including decoupling)
Conflict	Identify, eliminate, and/or reconcile
Gap	Identify, eliminate, and/or reconcile
Leverage Point	Identify & exploit

As summarized in Table 1, categorizing the range of possible 3S interactions also introduces opportunities to improve A/SMR design processes. One of the most impactful implications of the ongoing Sandia 3S research is this explicit relationship between potential 3S interaction and an associated system engineering design goal [11]. That Sandia's 3S approach is based on systems theory principles and complex system engineering introduces a mechanism to include 3S interactions into A/SMR design processes. The value of this result is bolstered by increasingly popular discussions of "by-design" approaches to mitigate international safeguards [12,13] and security [14,15] concerns and efforts to improve performance at safety/security interfaces [16,17]. Explicitly identifying—and designing for—3S interactions offers a broader solution space within which to creatively increase the effectiveness of A/SMR facility designs. To the extent these creative design decisions takes advantages of functional synergies, the underlying 3S approach also improves the efficiency A/SMR facility design.

A 3S-informed design approach, provides the framework for trade space analysis within systems engineering to trace the origins of negative interactions to either implementation, design, or requirements decisions. From a complex system engineering perspective, design decisions are focused on improving system performance, reducing the risk of poor system performance or (ideally) a combination of the two (Table 2). In an A/SMR context, nuclear safety, security and safeguards design can be reframed in terms of making decisions to reduce the possibility space for an undesired outcome or performance. And, as suggested by the Sandia 3S approach, engineering both individual "S" components and the interactions between them produces a larger solution space for A/SMR design. Consider how increased 3S interdependence produces more complexity within A/SMR operations—often resulting in higher likelihood of unexpected behaviors. To the extent such outcomes manifest, the benefit to better characterizing 3S interdependencies in design is the ability to apply related system engineering design goals. Here, for example, any increase in risk from 3S interdependence can be address by either decoupling (where possible) technical or infrastructural dependencies or reconciling such dependencies with procedures or policies.

Two of the other three 3S interaction types drive risk reduction via systems engineering design goals in a similar manner. For example, conflicts increase the potential for undesired A/SMR outcomes from negative interactions between safety, security and safeguards. In response, associated systems engineering design goals are to identify, eliminate (likely via technical, infrastructural or operational redesign) or reconcile (likely through regularly practiced and updated personnel procedures). Consider the tension between economic pressures to reduce facility-level security budgets and the need to maintain adequate protection against the DBT described in example 2.1. Where gaps produce undesired A/SMR outcomes from missing 3S interactions, the necessary systems engineering design goals are similar to those for conflicts. Yet, either the technical, infrastructural or operational redesign to eliminate or the regularly practiced and updated personnel procedures to reconcile gaps will focus on adding something to A/SMR design. Consider example 2.3, above, and the discussion about revisiting traditional VAI approaches to ensure certain failure modes and mechanisms are included in security discussions.

Lastly, leverage points represent a type of interaction that is less focused on risk reduction and more improving A/SMR performance. The extent to which design decisions to meet a given objective of one "S" simultaneously meets an objective for a different "S" indicates an improvement in effectiveness and efficiency. More pointedly, where such outcomes manifest, a given A/SMR design is able to accomplish the same objective with fewer (e.g., shared) resources. As such, the associated systems engineering design goals are to identify and exploit—which can include taking advantage of previously unidentified leverage points and redesigning to introduce new ones. The opportunities (and challenges) posed to safety, security and (international) safeguards from new, novel fuel forms—as described in example 2.3—are illustrative of potential leverage points in A/SMRs.

TABLE 2. SUMMARY RESULTS FROM APPLYING SANDIA'S SYSTEMS ENGINEERING DESIGN-BASED 3S APPROACH TO A/SMR EXAMPLES.

A/SMR Example (Section)	Safety	Security	Safeguards	[3S Interaction Type] Systems Engineering Design Goal
(2.1)	Capturing increased role of "less-critical" facility components as potential targets for malicious actions	Co-locating "critical" facility components to reduce security system footprint	(Similar challenges can be expected when considering fewer resources to support safeguards obligations)	[Conflict] Identify & reconcile → Security designs can incorporate facility/reactor physics
(2.2)	Verifying the burnup of each pebble/concentration of liquid fuel during rotation for efficiency	Accounting for/locating each pebble or amount of liquid fuel to prevent potential use as RDD	Confirming location of pebbles/liquid fuel to prevent diversion	[Leverage points] Identify & exploit → Selected measurement solutions for process monitoring can support actinide accounting &/or asset tracking
(2.3)	Implementing traditional PSA-approaches can neglect important elements of A/SMR operational risk	Conducting traditional VAI techniques propagate/compound these missing elements of operational risk	(Similar challenges might be expected when acquisition pathway analysis borrows from traditional adversary path analysis)	[Gaps] Identify & eliminate → New VAI approaches should be able to include passive safety systems & conducted earlier in the facility design process

As first demonstrated in [9,10], the A/SMR examples in Section 2 highlight some benefits for improving risk reduction by addressing 3S interfaces. Consider, for example, how categorizing 3S interface types—such as interdependencies, conflicts, gaps, and leverage points—helps invoke engineering design processes. Second, including behaviours *at* the 3S interfaces seems to better align with real-world operational uncertainties, including the anticipated multi-modal, multi-jurisdictional A/SMR deployment. And, by extension, 3S interface-informed risk reduction strategies can be designed to account for interdependencies not included in traditional independent "S" assessments and produce better A/SMR performance, as summarized in Table 2.

4. CONCLUSIONS, INSIGHTS & IMPLICATIONS

While traditional approaches that seek to optimize either nuclear safety or security or safeguards may yield apparent improvements in risk reduction, following tradition to do so in isolation disregards key aspects of integrated operational risk that can significantly impact overall performance. In addition, several anticipated characteristics of A/SMR design and development—including novel fuel forms, new operational procedures and

more remote deployment locations—further demonstrate the need for taking advantage of 3S interactions. An ability to categorize these interactions and align related A/SMR facility design goals is a strong step in this direction.

In response, Sandia has incorporated system theory principles and complex systems engineering concepts into an approach to provide a common mental model by which to coordinate between safety, security and (international) safeguards "by-design" decisions for anticipated A/SMR operations. As summarized in Table 2, several key impacts emerge from explicitly analyzing 3S interactions. For example, if A/SMR operation risk are assumed to be independent, then mitigation efforts should address different types of interdependencies—including conflicts, gaps, and leverage points. Similarly, applying systems theory principles and complex systems engineering concepts help align these different types of interdependencies to potential facility design performance objectives. Based on experience from research projects and U.S. vendor design engagements (and summarized in examples 2.1, 2.2, and 2.3), Sandia has demonstrated how making A/SMR design decisions is enhanced when accounting for interdependencies—whether between elements of 3S risk itself or between historically isolated 3S mitigations against such risk.

Sandia will continue to explore how to address each type of interdependency effectively and efficiently throughout the A/SMR design and development cycle. Lessons learned and insights gained form the foundation for additional investigation in several associated areas—including (but not limited to), mechanisms for 3S-informed policy/regulatory development, frameworks to develop international 3S best practices and "by-design" approaches to enhance decision processes for potential vendors, operators and hosts of A/SMRs.

ACKNOWLEDGEMENTS

This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government. Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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. **SAND2022-XXXX C**.

REFERENCES

[1] WORLD INSTITUTE FOR NUCLEAR SECURITY, WINS 2019 Annual Report: The Golden Threat of Nuclear (2019), https://wins.org/wp-content/uploads/2019/03/WIN-102-

[2] 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 (Abb. Ver.), National Academies of Science, Washington, DC, 2011

[3] HEINONEN, O., Nuclear Terrorism: Renewed Thinking for a Changing Landscape (2017),http://www. defenddemocracy.org/media-hit/olli-heinonen1-nuclear-terrorism-renewed-thinking-for-a-changing-landscape/

[4] EVANS, A., HOROWITZ, S., EVANS, C., STROMBERG, B., and KNUDSEN, R., U.S. Domestic Pebble Bed Reactor Security by Design (SAND2021-13122R), Sandia Nat. Lab., NM, USA, 2021.

[5] PRECISION REMOTES, Nuclear Power Plant Defense – The Future of Nuclear Security Technical Impacts and Increased Operations Safety (2022), https://www.precisionremotes.com/nuclear-power-plant-solutions

[6] GIBBS, P., HU, J., KOVACIC, D., AND SCOTT, L., Pebble Bed Reactor Domestic Safeguards, FY21 Summary Report (ORNL/SPR-2021/169124) Oak Ridge Nat. Lab., TN, USA, 2021.

[7] DION, M.P., GREENWOOD, M.S., HOGUE, K.K., O'BRIEN, S.E., SCOTT, L.M., AND WESTPHAL, G.T., MC&A for MSRs: FY2021 Report (ORNL/SPR-2021/2305) Oak Ridge Nat. Lab., TN, USA, 2021.

[8] WHITEHEAD, D. and VARNADO, G., Vital area identification for U.S. Nuclear Regulatory Commission nuclear power reactor licensees and new reactor applicants (SAND2008-5644), Sandia Nat. Lab., NM, USA, 2008.

[9] WILLIAMS, A. and OSBORN, D., System Studies for Global Nuclear Assurance & Security: 3S Risk Analysis for Small Modular Reactors (II)—Conclusions & Implications (SAND2018-14164), Sandia Nat. Lab., NM, USA, 2018.

[10] WILLIAMS, A. and OSBORN, D., System Studies for Global Nuclear Assurance & Security: 3S Risk Analysis for Portable Nuclear Reactors (II)—Conclusions & Implications (SAND2020-4688), Sandia Nat. Lab., NM, USA, 2020.

[11] WILLIAMS, A., Systems theory principles and complex systems engineering concepts for protection and resilience in critical infrastructure: lessons from the nuclear sector, INSIGHT Magazine **23** 2 (2020) 14-20.

[12] WHITLOCK, J., "Safeguards considerations for microreactors," IAEA Tech. Mttg Microreactors, Austria, 2021.

[13] BARI, R. and CHENG, L., Outreach to Industry on Safeguards by Design Concept for Small Modular Reactors (Rep.#222920-2022), Brookhaven Nat. Lab., NY, USA, 2022.

[14] WORLD INSTITUTE FOR NUCLEAR SECURITY, 4.1 Implementing Security by Design at Nuclear Facilities (2019), https://www.wins.org/document/4-1-security-by-design/

[15] EVANS, A., WILLIAMS, A., and HOLT, K., A licensing & engineering security-by-design model for advanced & small modular reactors, Proc. of INMM Annual Meeting (2022), NJ, USA.

[16] U.S. NUCLEAR REGULATORY COMMISSION, Regulatory Guide 5.74: Managing the Safety/Security Interface, U.S. NRC, MD, USA, 2015.

[17] BUSQUIM E SILVA, R., PIQUEIRA, J., CRUZ, J. and MARQUES, R., Cybersecurity assessment framework for digital interface between safety and security at nuclear power plants, Int. J of Crit. Infra. Prot., **34** (2021).