SAND2021-9800C

Proceedings of the INMM & ESARDA Joint Virtual Annual Meeting
August 23-26 & August 30-September 1, 2021

A SYSTEMS-THEORETIC FRAMING FOR AN INTEGRATED NUCLEAR ENERGY SAFETY, SAFEGUARDS, AND SECURITY (3S) APPROACH

Adam D. Williams, Benjamin B. Cipiti, Alan Evans
Sandia National Laboratories*
Albuquerque, NM, USA, adwilli@sandia.gov

ABSTRACT

To support the successful—and peaceful—implementation of advanced nuclear reactors (AR) and small modular reactors (SMR), there is a need apply technologies, training, policies, and protocols to meet safety (e.g., preventing unintentional radiological releases), safeguards (e.g., preventing military use of nuclear technologies), and security (e.g., protecting against intentional radiological release or theft) objectives. Yet, in the words of former Deputy Director-General for Safeguards at the International Atomic Energy Agency Olli Heinonen "Safeguards, security, and safety are commonly seen as separate areas in nuclear governance…[though] Each has a synergetic effect on the other…[that] contribute to the effectiveness of the nuclear order."

As a response, current research at Sandia National Laboratories (Sandia) has investigated how systems theory principles and complex systems engineering concepts frame the complexities of interactions between traditional safety, safeguards, and security in the nuclear sector. For example, this research suggests there is a significant benefit from viewing nuclear security as an emergent property that is influenced by its interactions with well-understood nuclear safety processes and international safeguards regimes. This Sandia research indicated some key benefits from explicitly incorporating interactions into the analytical framework, namely in terms of bettering identifying interdependencies, conflicts, gaps and leverage points across traditional safety, security, and safeguards hazard mitigation strategies.

After introducing how key concepts in systems theory provide a logical framework to capture interactions between safety, safeguards, and security in nuclear activities, this paper will describe an approach that Sandia has employed to explore the risk complexity from these interactions. Next, this paper will summarize and describe the results of applying this approach to several nuclear energy-related case studies—spent nuclear fuel transportation, small modular reactors, and portable nuclear power reactors. Lastly, this paper will discuss the conclusions, insights, implications, and next steps of Sandia's systems-theoretic framing for an integrated nuclear energy safety, safeguards, and security approach.

INTRODUCTION

* SAND2021-TBD C. 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.

Traditionally, nuclear reactors and fuel cycle facilities have focused on analyzing safety, security, and (international) safeguards (each one of the "3S's") separately. There are several reasons for this historical approach. For example, very large reactors nuclear sites have a large spread in buildings and functions. Dedicated safety systems can be distributed across different vital areas, safeguards requirements for material balance areas also may spread out over different buildings, and security requirements need to encompass the entire spread of the site. The large facility size has led to more separation in the systems. There is also a regulatory history supporting the need for separation of duties and functions among these performance-based attributed of nuclear facilities. Lastly, historical separation of the 3S's has also been driven by sponsored research being limited to focus on only one of these domains. An international safeguards sponsor, for example, does not necessarily look to fund research on nuclear safety in support of its nonproliferation-related mission. A research program focused on safety of advanced reactors (AR) likely is not interested in funding research on cybersecurity. For these reasons (and others) finding support for funding exploration into the observed interactions across safety, security, and (international) safeguards—so-called "3S analysis"—has been a challenge.

Despite the challenges, the move toward smaller, modular, and potentially safer ARs and SMRs require re-examining these constraints and revisiting the opportunities for (and potential benefits of) 3S analysis. SMRs, and particularly the move toward microreactors, physically places all the reactor functions in a small space, so there is more overlap between safety, safeguards, and security (see Figure 1). To aid in SMR economic justification, reactor vendors also want to reduce on-site presence of staff in order to compete better with other sources of power. This is potentially a tectonic shift in nuclear power operations as these facilities would not have the luxury of separate safety, security, and (international) safeguards staff functions with only tens of personnel on site. The move toward "inherently safe" designs could also lead to new regulatory options that would benefit from more integrated thinking between the 3S's. Taken together, a 3S approach seems well poised to better address the challenges facing—and enhance the potential benefits of—small modular reactors.

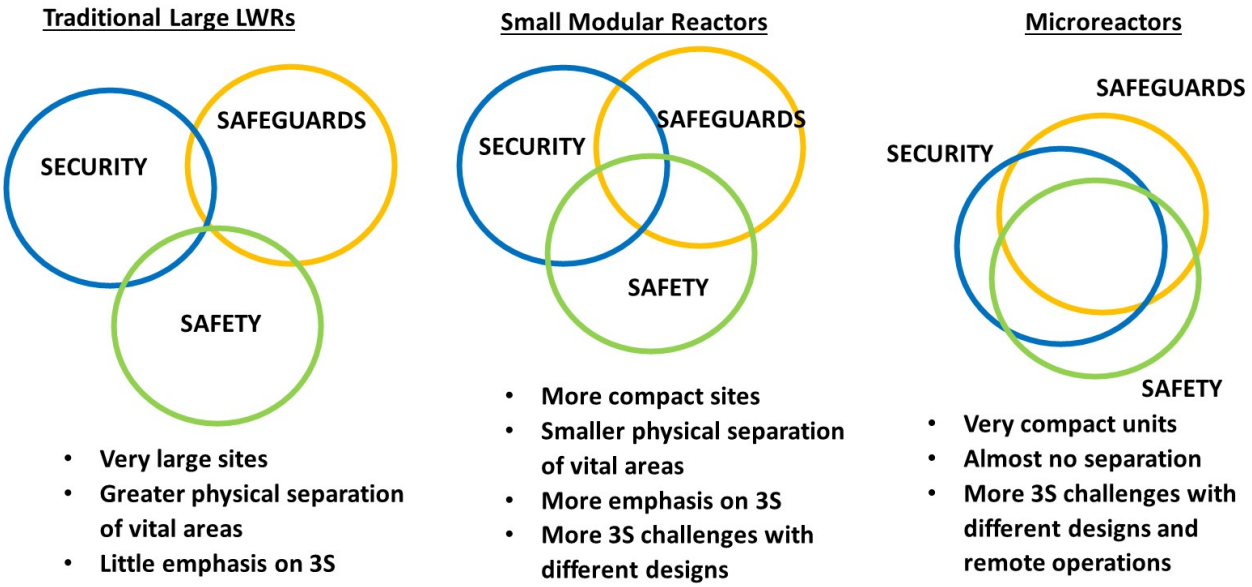


Figure 1. Conceptual illustration of the increasing overlap of the 3S's as reactor size decreases

Described more succinctly by former Deputy Director-General for Safeguards at the International Atomic Energy Agency Olli Heinonen:

> *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 [1]. (Emphasis added)

BACKGROUND

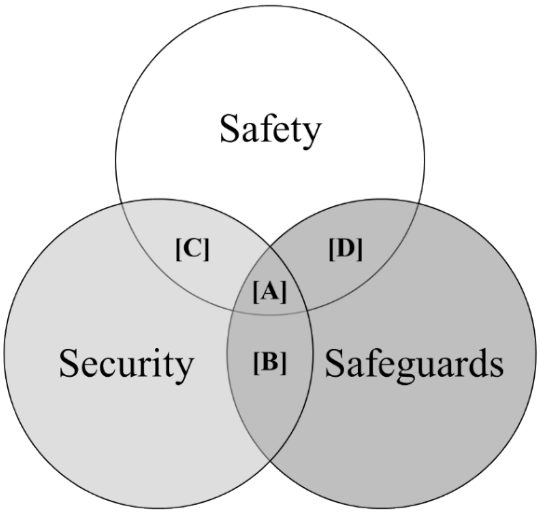
Sandia has invested in developing capabilities to better identify and characterize these interdependencies between safety, safeguards, and security. More specifically, technical evaluation funded under Sandia's *Global Nuclear Security and Assurance* (GNAS) initiative has sought to anticipant, assess, and address nuclear risks using advanced systems, technologies, expertise, and situational awareness tools. Conclusions from this work reframes the discussion around the risk complexity for nuclear fuel cycle activities to provide a new way to explore these interdependencies. The emphasis of this work, therefore, is not to select specific technical widgets or determine detailed procedures to enhance safety, security, and (international) safeguards. Rather, the GNAS point of emphasis for 3S analysis is to identify—and ideally influence—facility design performance parameters to reduce risk complexity and improve operational efficiency [2,3].

These Sandia conclusions helped shape three useful insights for evaluating risk complexity in safety, safeguards, and security for SMRs. First, an integrated 3S approach can help identify gaps, interdependencies, conflicts, and leverage points across traditional standalone safety, security, and safeguards analysis techniques. This borrows heavily from a systems-theoretic perspective to better understand the actual impacts of interactions in order to explicitly include them in design decision-making. Second, including the interdependencies between safety, safeguards, and security better aligns with real-world operational uncertainties observed in multi-jurisdictional systems. Many of the marketed characteristics of SMRs suggest more sources of uncertainty, including remotely located and (possibly) more transportable operational environments. Lastly, risk mitigation strategies resulting from integrated 3S risk assessments can be designed to better account for interdependencies not included in independent "S" assessments.

ARs and SMRs have seen a resurgence of interest over the past decade mainly driven by increased private and venture capital money going into new reactor designs. These efforts have been further supported by the U.S. Department of Energy's Advanced Reactor Demonstration Program (ARDP) area which provides cost-share support to several vendors to encourage deployment of ARs. Encouragingly, many of the vendors recognize the importance of safety, security, and (international) safeguards (often conflated with "non-proliferation") on the future viability of the AR and SMR products. Additionally, there seems to be a growing recognition of the value of a more integrated approach to managing related risk complexity—sometimes referred to as a safety, security, and safeguards by design (3SBD)—early in the design process.

INTEGRATED 3S AS A FUNCTION OF SYSTEMS THEORY CONCEPTS

Sandia's GNAS studies demonstrate how systems theory principles and complex systems engineering concepts help frame the complexity in—and *interactions* between—nuclear safety, safeguards, and security in real-world operations. Such systems theory principles as hierarchy (functional descriptions of levels of complexity within a system), emergence (the observed phenomena by which behaviors at a given level of complexity are irreducible to and inexplicable by the behavior of component parts), and interdependence (interactions and influences that impact the ability of systems to achieve their desired objectives) help describe safety, safeguards, and security for SMRs. Current systems engineering efforts are combining these systems theory principles to design and operate ever increasingly complex systems. As this is observed, then engineering for SMRs should be cognizant of—if not explicitly incorporate—3S risk mitigation processes that form part of its operational environment. Complex systems engineering offers the mechanism by which to better address the multidomain interdependencies between long-established nuclear safety practices, internationally-mandated nuclear safeguards processes, and socio-technical nuclear security systems. Examples of 3S interactions and representative examples are illustrated in Figure 2.



3S Interaction	Representative Example [Location on Venn Diagram]
Interdependency	Coordination of 3S responsibilities during emergency operations [A]
Conflict	Intrusive access control could impede evidence of peaceful uses (*increase safeguards risk*) [B]
Gap	Passive safety systems could be new targets for malicious acts (*increase security risk*) [C]
Leverage Point	Safeguards inspections could reveal a reactor vessel integrity issues (*reduce safety risk*) [D]

Figure 2. Types of interactions between safety, security, and safeguards in the critical nuclear infrastructure sector, with representative examples, recreated from [4].

Other efforts in the nuclear sector have taken a range of approaches to explore 3S integration that range from calls for using shared video surveillance data between safety, safeguards, and security to pairing the traditional security-related issue of sabotage with safety and traditional security-related issue of theft with safeguards. In contrast, the Sandia 3S studies employed systems theory and complex system engineering to better capture these interactions and identify related systems design goals—whether between risks and mitigations (interdependencies), characterize oppositional forces in operational risks (conflicts), identify missed operational risks (gaps), and capture natural redundancies or compensatory effects to mitigate risks (leverage points).

Table 1. Summary of systems engineering design goals for each type of interaction evaluated in Sandia's systems-theoretic approach to nuclear safety, security, and safeguards.

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

Four types of 3S interactions were captured in these Sandia studies, as well as related systems engineering design goals (Table 1). For example, where interdependencies refer to aspects of expected individual "S" operations whose operations are directly impacted by the behavior from operations in another "S," Sandia's 3S analysis can help identify interactions within SMRs that may impact—either positively or negatively—expected safety, safeguards, or security behaviors. Or, consider conflicts, which refer to aspects or objectives of expected individual "S" operations that negatively overlap with expected behaviors from a different "S." A 3S design approach, in response, employs various forms of trade space analysis within systems engineering to trace the origins of negative interactions to either implementation, design, or requirements decisions. Similarly, consider another type of negative interactions that capture troubling operations or behaviors that have not yet been identified. As such, gaps refer to aspects or objectives of expected individual "S" operations that are not captured, mitigated, or otherwise addressed and yield opportunities to develop innovative solutions to improve system behaviors. The last type of interaction captured in these Sandia studies—leverage points—refer to aspects or objectives of expected individual "S" operations that positively overlap with expected behaviors from a different "S." These serve as potential "force multipliers" between safety, safeguards, and security when an improvement in one "S" results in a simultaneous improvement in expected behaviors in another "S."

Ultimately, these identified systems engineering design goals help reinforce the concept that 3S interdependence can be *desired*. For example, consider the multiple responsibilities involved when SMRs might be in transit and must cross a national (or international) border. Due to the

need to adhere to all safety, safeguards, and security responsibilities along the entire movement route of the SMR, border crossings represent a transition in risk mitigation responsibility that can stretch traditional inspection approaches. For such a hypothetical SMR example, aspects of (international) safeguards inspections could be assigned to safety inspectors to take advantage of the larger number of qualified safety inspectors worldwide. Thus, the need to meet continuity of knowledge responsibilities for SMRs is enhanced by designing jurisdictional transition inspections to leverage data commonly collected for safety purposes to meet (international) safeguards obligations. Explicitly identifying—and designing for—interdependencies provides opportunities for better leveraging resources toward "force multiplier" decisions on facility design performance parameters.

3S EVALUATION: REPRESENTATIVE CASE STUDIES

To better demonstrate the potential value of a 3SBD approach for civilian nuclear power projects—including SMRs and ARs—the following two case study summaries are presented. The first example discusses U.S. AR deployment and focuses on some challenges faced by vendors related to licensing. The second focuses on international security-by-design for future SMR deployment. These cases are not offered as comprehensive proof, but rather as representative demonstrations to support additional intellectual, empirical, operational, and policy-based investigation into 3SBD approaches.

Representative Example 1: U.S. Domestic Licensing of AR

In the U.S., regulatory requirements for licensing nuclear reactors were developed to support large-scale, light water reactor (LWR) based nuclear power plants (NPP). Given the different physical scale and technological scope between such traditional NPPs and AR/SMRs, the 3S requirements may differ. Particularly when considering the changes in timescales and multi-stakeholder nature related to the different fuels, refueling patterns, source terms, and physical sizes of AR/SMRs. In navigating this ongoing alignment between current "S" regulatory requirements, vendors may need to ask for exemptions to progress along their AR/SMR timeline—which potentially adds uncertainty to the licensing process.

One specific challenge AR/SMR may vendors face relates to meeting physical protection goals in a cost-effective manner. Consider, for example, a regulatory requirement for a fixed number of on-site responders. The associated resource costs to meeting such a regulatory requirement could make smaller footprinted AR/SMR-based plants economically uncompetitive since the costs would be proportionally higher than LWR-based NPPs. In addition, such requirements may not be appropriately matched to AR/SMR plants with smaller source terms—and therefore smaller potential radiological consequences.

In response to this—and similar issues—the U.S. Nuclear Regulatory Commission (NRC) is going through rulemaking to help improve the licensing process for ARs [5]. While specific details are being worked out, the new rule-making follows a risk-informed approach. For example, AR/SMR vendors will have additional options to meet security requirements, including for Physical Protection System (PPS), as long as dose at the site boundary is below a regulated threshold. Therefore, inherently safe reactor designs proven to keep the resulting dose of any accident (or sabotage scenario) below that mandated threshold can be leveraged to support security requirements. This could include a PPS with a much smaller on-site responder presence.

Similarly, AR/SMR plants may increasingly utilize local law enforcement resources as more effective detection and delay features (which are often more economical than additional detection components) are added or if accident sequence timelines are taken into account.

In order to take advantage of these leverage points being considered under new rule-making, AR/SMR vendors could benefit from an integrated 3S approach[1]. Security analyses need to understand all potential sabotage pathways, which in turn requires a deep understanding of the safety features within the AR/SMR facility. More specifically, higher fidelity timelines for sabotage scenarios could incorporate safety accident progression timelines. Here, the ability of AR/SMR security to provide enough delay to stop the attack using local law enforcement resources or recover after a sabotage event before a consequence that surpasses the off-site dose limit is directly improved with better safety systems. While the tools to provide the safety and security analyses exist separately, there seems to be some distinct benefits to be experience from more integrated or blended approaches for AR/SMR vendors. The Advanced Reactor Safeguards program, funded through the U.S. Department of Energy, is providing research and analyses to examine this interface between security and safety.

Representative Example 2: International SMR Security-by-Design

The international community has expressed increasing interest in pursuing SMR technology for reliable power generation, desalination, district heating and other applications. Among other anticipated benefits, the deployment of SMRs is being considered for their potential cost savings. International interest is also driven by SMRs that have redundant safety systems and multiple reactors—which also increases the number of target sets that a physical security system must protect. This requires a complete integration and collaboration with reactor designers, site personnel and operators, and the security group for successful international SMR deployment to meet cost savings and safety goals. For example, consider security system designs that allow for a reduced onsite response force or more heavily leverage an offsite response force (e.g., local law enforcement agency) and still meet security performance requirements.

SMRs are currently being designed with robust safety features that lead to the inherent (or passive) safety systems for the site to reduce overall operational risk. For successful SMR deployment, it is important that security designs and safety considerations are integrated in such a way that reactor operations and safety systems are adequately protected. Such integration is key for reducing an onsite response force and potentially reducing the cost of the security system over the lifetime of the plant. Yet, developing such a security system requires complex integration of detection and assessment technologies, access delay barriers, and an offsite response force with SMR operations. For demonstration, consider a detailed analysis of a hypothetical SMR with redundant safety systems [6]. In this example, the security system was designed with increased physical barriers onsite (e.g., additional walls), increased detection along the perimeter of the facility (e.g., vibration sensors), and the application of active delay barriers (e.g., obscurants and slippery agents). While these attributes are not novel, their

[1] The authors understand that this representative example does not explicitly include (international) safeguards. This was purposeful to address more urgent safety and security concerns for AR/SMR vendors to program toward U.S. licensing. The overall logic, however, easily extends to including (international) safeguards considerations, which may improve attractiveness of AR/SMR designs in international markets.

implementation into SMRs to provide an integrated and advanced security system to adequately protect SMR operations and safety systems to help meet cost savings is a cutting-edge application of a 3S approach.

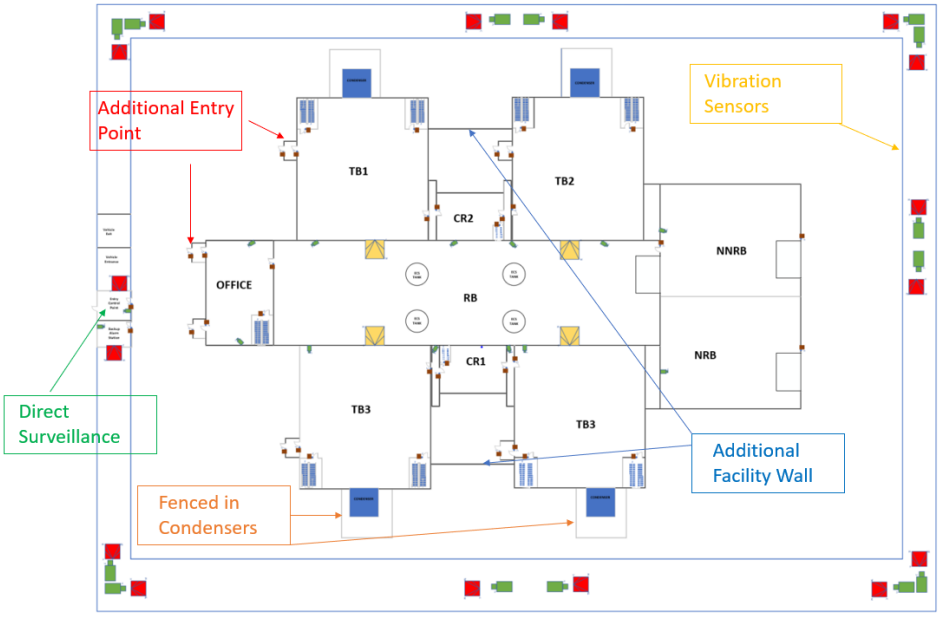


Figure 1. Security-by-Design schematic for a hypothetical SMR, from [5]

From this study many insights were gained for the integration of security and safety into the design of SMR facilities. These insights include [6]:

- Protecting necessary target sets by physical separation in the plant design phase—a common safety practice—will increase adversary task time leading to an effective security system
- Coordination between reactor designers and safety personnel can ensure accurate identification of target sets
- Security system design and facility design can increase the effectiveness and operational efficiency at an SMR site

CONCLUSIONS

As illustrated in the two representative case study summaries, several dynamics and trends related to AR/SMR development and deployment support 3SBD approaches. Both examples highlight potential benefits of explicitly accounting and designing for interdependencies—which include opportunities to leverage safety systems to support reduced on-site security staff or increasing physical separation for safety increases adversary task time. AR/SMRs will introduce new challenges to designing and implementing resilient facilities and systems capable of meeting safety, security, and (international) safeguards needs among increasingly complex operational environments. While traditional approaches that seek to optimize *either* nuclear safety or security or (international) safeguards may yield *apparent* improvements in risk reduction, doing so disregards key aspects of risk complexity that can significantly impact overall performance. In addition, AR/SMR development clearly demonstrates that need for logical consistency between changes in regulatory rule-making and changes in risk analysis and mitigation techniques.

Yet, recent work at Sandia supporting both domestic and international missions demonstrated the impacts and implications of exploring the *interactions* between safety, security, and (international) safeguards to enhance risk mitigation for AR/SMRs. Several important implications resulted from these conclusions. First, risks for AR/SMRs are not necessarily independent—implying that protection and resilience efforts should address the potential for interdependency. Second, systems theory principles provide a useful lens framing for interdependencies and complex systems engineering concepts provide mechanisms for characterizing potential facility design performance parameters. Third, evaluating interdependencies, conflicts, gaps, and leverage points helps incorporate elements of the operational environment into AR/SMR plant design—a likely increasing source of notable uncertainty as these facilities are deployed to increasingly remote locations. Lastly, designing risk reduction strategies is enhanced when accounting for interdependencies—whether between elements of 3S risk itself *or* between historically isolated 3S mitigations against such risk.

As demonstrated, invoking system theory principles and complex systems engineering concepts helps provide a common mental model by which to coordinate multi-domain risk mitigations toward the same protection and resilience goals for anticipated for AR/SMR operations. Sandia continues to explore these interdependencies and provide unique capabilities to support research in all these domains. These lessons and insights imply support for additional investigation in several associated areas—including, but not limited to, mechanisms for 3S integration in policy/regulatory development, better incorporation of (international) safeguards-related risks, and design approaches to enhance AR/SMR designs to be more consistent with domestic and international 3S best practices.

REFERENCES

[1] O. Heinonen, "Nuclear Terrorism: Renewed Thinking for a Changing Landscape," <http://www.defenddemocracy.org/media-hit/olli-heinonen1-nuclear-terrorism-renewed-thinking-for-a-changing-landscape/>, 2017.

[2] A. D. Williams and D. Osborn, "System Studies for Global Nuclear Assurance & Security: 3S Risk Analysis for Small Modular Reactors (Volume II)—Conclusions & Implications (SAND2018-14164)," Sandia National Laboratories, Albuquerque, NM, 2018.

[3] A. D. Williams and D. Osborn, "System Studies for Global Nuclear Assurance & Security: 3S Risk Analysis for Portable Nuclear Reactors (Volume II)—Conclusions & Implications (SAND2020-4688)," Sandia National Laboratories, Albuquerque, NM, 2020.

[4] A. D. Williams, "Systems Theory Principles and Complex Systems Engineering Concepts for Protection and Resilience in Critical Infrastructure: Lessons from the Nuclear Sector," *INSIGHT Magazine*, INCOSE, 23(2), pp. 14-20, 2020.

[5] "Risk-Informed, Tehchnology-Inclusive Regulatory Framework for Advanced Reactors—A Rule Proposed by the Nuclear Regulatory Commission," Federal Register, <https://www.federalregister.gov/documents/2020/11/06/2020-24387/risk-informed-technology-inclusive-regulatory-framework-for-advanced-reactors> , 2020.

[6] A. Evans, C. Evans, J. Parks, S. Horowits, R. Knudsen, "International Small Modular Reactor Physical Protection System Design and Analysis." Sandia National Laboratories. SAND2020-13264