SAND2023-03995C

Proceedings of the INMM & ESARDA Joint Annual Meeting
May 22-26, 2023

SYSTEMS ENGINEERING FOR INTERNATIONAL NUCLEAR SAFEGUARDS

Adam D. Williams
Sandia National Laboratories*
Albuquerque, NM, USA, adwilli@sandia.gov

ABSTRACT

Anticipated changes to traditional civilian nuclear markets—namely those stemming from advanced and small modular reactors (A/SMR)—will introduce new and novel challenges to the international safeguards regime. More specifically, some experts have described how new nuclear fuels, fuel cycles and spent fuel management systems will challenge the ability for timely and effective safeguards verification for A/SMRs. Traditionally, safeguards solutions have been developed by domain experts in nuclear material measurements, physical and electrical containment, electrical surveillance and area/environmental radiological signal monitoring. Yet, the uncertainty (and complexity) of achieving comparable levels of safeguards success with the anticipated challenges related to A/SMR deployment suggest the need for additional areas of technical expertise.

Systems engineering, defined as "a transdisciplinary and integrative approach to enable the successful realization, use, and retirement of engineered systems, using systems principles and concepts, and scientific, technological, and management methods" by the International Council on Systems Engineering (INCOSE) seemingly provides the logical and technical acumen to address these challenges to international nuclear safeguards. Building on recent discussions with international safeguards experts, this concept paper seeks to explore the efficacy of visualizing international nuclear safeguards through a systems engineering lens, which includes (but is not limited to): describing traditional nuclear safeguards in terms of emergent behaviors, reconceptualizing traditional nuclear safeguards objectives as functional requirements and addressing key points of interdependence within traditional nuclear safeguards approaches. The result is a notional systems engineering-based framework for international nuclear safeguards aimed to mitigate a representative set of the previously described challenges.

After summarizing today's international nuclear safeguards regime and describing forecast challenges from A/SMR deployment, this paper will introduce INCOSE-defined elements of systems engineering. Building on this systems engineering perspective for international safeguards, this paper will then explain how such a framing of nuclear safeguards can mitigate anticipated near-term challenges. Lastly, this paper will discuss conclusions and insights for the adequacy of systems engineering to improve international nuclear safeguards, as well as implications for next steps toward furthering this exploration and for inclusion in "3S-by-design" approaches.

INTRODUCTION

Anticipated changes to traditional civilian nuclear markets—namely those stemming from advanced and small modular reactors (A/SMR)—will introduce new and novel challenges to the international safeguards regime. Traditionally, safeguards solutions have been developed by domain experts in nuclear material measurements, physical and electrical containment, electrical surveillance and area/ environmental radiological signal monitoring. For example, the most common measures for implementing international safeguards obligations include (Table 1):

- nuclear material accounting (NMA)
- containment and surveillance (C/S)
- design information verification (DIV)
- environmental sampling (ES)
- complementary access (CA)
- open-source analysis (OS)

Decades of experience and lessons learned have helped to optimize how specific mechanisms within each of the safeguards measures listed above are applied to civilian nuclear materials uses across the globe.

Yet, the uncertainty (and complexity) of adequately implementing safeguards with the anticipated challenges related to A/SMR deployment are starting to present themselves in two higher-order categories: challenges unique to A/SMR concepts of operations and broader challenges to international safeguards that may be amplified by A/SMRs. For example, the following technical characteristics associated with different A/SMR designs "potentially impact the implementation of international safeguards": low thermal signatures, remote locations (with limited access), many reactor sites spread over a large geographical area, long-life reactor cores, advanced fuel cycles (including fuels with higher uranium enrichment), excess reactivity, different fuel element sizes, new spent fuel storage geometries, novel fissile inventories and unique environmental consideration [1].

More specifically, some experts have described how new nuclear fuels, fuel cycles and spent fuel management systems will challenge the ability for timely and effective safeguards verification for A/SMRs (and related fuel cycle activities). For example, consider how NMA safeguards activities for traditional light water reactors (LWR) are well established—including well-established (non)destructive assay measurements at key measurement points and robust C/S systems. In contrast, coupling the anticipated plans to deploy A/SMRs remotely with many designs using high-assay, low-enriched uranium (HALEU) potentially makes such NMA activities as random sampling, inventory taking, and other measurements more costly and time intensive for the International Atomic Energy Agency (IAEA) to execute. Similarly, the existence of new material characteristics in A/SMR fuel cycles suggests needs for advances in C/S to mitigate wider use of HALEU and monitoring new potential plutonium (Pu) pathways.

Table 1. Descriptions of (and representative examples for) common international safeguards measures

	Standard Definition from "IAEA Safeguards Glossary" [2]	Representative example activities or system elements
Nuclear Material Accounting [NMA]	"The practice of nuclear material accounting as implemented by the facility operator and the State system of accounting for and control of nuclear material (SSAC), inter alia, to independently verify the correctness of the nuclear material accounting information in the facility records and the reports provided by the SSAC to the IAEA." "Activities carried out to establish the quantities of nuclear material present within defined areas and the changes in those quantities within defined periods."	• Near real time accountancy system • Non-destructive/destructive assays • Physical inventory taking • Material unaccounted for calculations • Shipper/receiver difference reports • Inventory verification (e.g., weighing, volume determination, sampling and analysis, criticality check, item counting • Complementary containment/surveillance measures & monitoring
Containment & Surveillance [C/S]	"Containment [includes the] structural features of a facility, containers of equipment which are used to establish the physical integrity of an area or items…to maintain the continuity of knowledge of the area or items … Surveillance [is] the collection of information through inspector and/or instrumental observation aimed at detecting movements of nuclear material or other items, and any interference with containment or tampering with IAEA equipment, samples[,] and data."	• Walls of the storage room • Transport flasks • Storage containers • Seals • Periodic examination • Optical surveillance devices
Design Information Verification [DIV]	"Activities carried out by the IAEA at a facility to verify the correctness and completeness of the design information provided by the State."	• Review of asset design drawings • Review of quality assurance monitoring reports • Spot checks
Environmental Sampling [ES]	"The collection of samples from the environment with a view to analysing them for traces of material that can reveal information about nuclear material handled or activities conducted."	• Location specific sampling • Swipe samples • Point samples • Composite samples • Scanning electron microscopy • Fission track analysis (thermal or secondary ionization mass spectrometry)
Complementary Access [CA]	"Access provided by the State to IAEA inspectors with the provisions of an Additional Protocol… the IAEA shall have complementary access for three purposes: to assure the absence of undeclared nuclear material and activities…where nuclear material has been declared to be present; to resolve a question relating to the correctness and completeness of the information…or to resolve an inconsistency relating to that information; to confirm, for safeguards purposes, the declaration of the decommissioned status of a facility or a location outside facilities where nuclear material was customarily used."	• Visual confirmation • Utilization of radiation detection and measurement devices • Application & inspection of seals and other identifying and tamper indicating devices • Examination of records relevant to Additional Protocol (AP) undertakings & specific expanded declarations
Open Source [OS]	"Analysis of information generally available to the public from external sources, such as scientific literature; official information; information issued by public organizations; commercial companies and the news media; and commercial satellite imagery."	• News sources • Social media • Trade data • Science & technology publications

		• Ship-tracking databases

In terms of DIV, the modularity and transportability of some A/SMR designs indicate a manufacturing strategy that could diminish the ability to confirm design, especially as such information may have been lost (physically or in translation) during the transfer from the supplier state to the host state. Projected deployment of multiple A/SMR units in increasingly remote locations may be obstacles for the efficacy of many ES techniques (e.g., swipe samples) and CA approaches (e.g., coordinating timely site visits)—challenging technical, procedural and operational norms developed under the current international safeguards regime. Lastly, OS capabilities will need to expand in scale and scope to best evaluate the increase in available data as A/SMRs meet forecast deployment plans. Though representative, the challenges associated with NMA, C/S, DIV, ES, CA, and OS related to A/SMR deployment suggest the need for additional areas of technical expertise.

In response, many of the anticipated A/SMR-related challenges to international safeguards seem associated with systems implementation and project management capabilities [3]. Where technical components need to be selected, implemented and operated in a coordinated manner to achieve safeguards objectives, there is benefit in exploring different elements that underly systems implementation. For example, safeguards technologies must be adequately tested in preparation for production and deployment. In addition, the selected and implemented technologies need to not only form an integrated safeguards systems themselves, but also should efficiently integrate into larger operational systems at nuclear facilities. Orchestrating lifecycle planning and supply chain options are also important considerations given that these technical components are expected to achieve safeguards objectives over their lifetimes. Though systems implementation consists of many more elements, those pertaining to integration (e.g., managing interactions and interfaces) and dynamism (e.g., operations over time) seem particularly germane to mitigating A/SMR-related challenges to international safeguards.

The project management discipline also offers concepts and tenets seemingly beneficial to addressing some of these projected challenges. If systems implementation helps navigate the technical space of these challenges, then project management helps navigate the operational and procedure space. For example, project management provides techniques and methodologies to enhance risk mitigation, which provides support to managing concerns to schedules and resource needs to meet A/SMR safeguards objectives. The project management discipline can also play a key role in ensuring any deployed safeguards technology is operated to the highest possible quality, where associated frameworks can help navigate multi-stakeholder and multi-jurisdictional considerations of some anticipated A/SMR deployment scenarios. This coordination helps ensure that deployed safeguards solutions are able to achieve their intended objectives in a manner valid and verifiable to the international community.

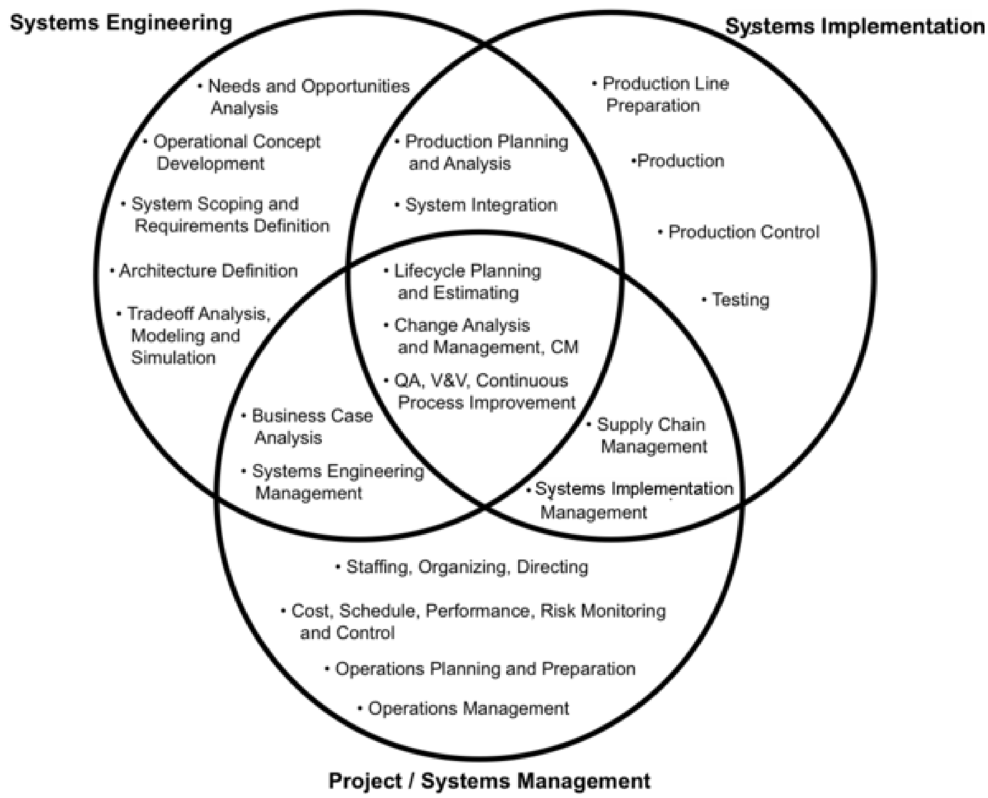

Figure 1. Venn diagram visualizing intersections of intellectual domains associated with systems engineering, from [3].

If individually the systems implementation and project management disciplines are advantageous for aligning potential next steps in international safeguards for A/SMRs, then taken together there are even more so. When considering blending elements of these two disciplines (Figure 1), the result is a more complete framing of international safeguards for A/SMRs. For example, new safeguards solutions for A/SMRs can be visualized more as architectures composed of interacting technological and procedural components. By incorporating procedural or operational considerations into the design of safeguards solutions, efforts to coordinate individual component and collective system behaviors are enhanced. More specifically, decisions on which capabilities to implement can be made by comparing the performance of an individual element versus the impact on the overall ability to achieve a safeguards objective. For example, a cutting-edge NMA technique may provide enhanced material monitoring capabilities for an A/SMR, but its digital-infrastructure needs might draw resources necessary for a C/S component to operate effectively. In this manner, invoking elements of these two disciplines in tandem offers an ability to navigate interfaces and interdependencies as trade-offs in the ability to meet international safeguards objectives.

SYSTEMS ENGINEERING: OPTIONS & OPPORTUNITIES

One intellectual discipline well-suited to address increased complexity, interdependencies, trade-offs and designing for emergent behaviors is *systems engineering*. Systems engineering is defined as "a transdisciplinary and integrative approach to enable the successful realization, use, and retirement of engineered systems, using systems principles and concepts, and scientific, technological, and management methods" by the International Council on Systems Engineering (INCOSE) [4]. INCOSE further advocates for the broadest interpretation of engineering—which includes "the action of working artfully to bring something about"—to describe the frameworks and techniques necessary to effectively coordinate desired behaviors from systems composed of (any or all) people, products, services, information, processes, and natural elements [4]. Consistent with the preceding argument that solutions combining elements of the systems implementation and project management disciplines provide additional performance-related advantages (Figure 1), consider the following description:

> Systems engineers are "and" people. They understand the "big picture" *and* the details. They communicate well with engineers *and* executives. They know how to analyze complexity *and* how to design for simplicity. They balance budgets *and* make technical trade-offs. They appreciate both the abstract *and* the concrete [5, pg. 1]

If engineering is to be considered the art of manifesting a solution, then a parallel (and equally broad) conceptualization of a system is necessary. According to INCOSE, the most basic definition of a system is "an arrangement of part or elements that together exhibit behaviour or meaning that the individual constituents do not [4]." More specifically, INCOSE asserts that a system can be of a *physical* or a *conceptual* nature. Components in physical systems consist of matter and energy and demonstrate observable behaviors—with such examples as space shuttles and nuclear power plants. In conceptual systems, components tend to be purely informational and demonstrate complex meaning—with such examples as economic markets and the international nuclear safeguards regime. Whether or physical or conceptual, all such systems display behaviors (or observed performance) that emerges from both the capabilities of individual components *and* the interactions between them [4]. As such, systems engineering then can be considered the art of working artfully to design for the interactions between components to achieve desired system-level performance outcomes.

As a practical extension, systems engineering leverages several key systems-theory principles and complex systems-engineering concepts. As previously indicated, the principle of *emergence* describes how interactions among system components (or with environmental influences) drive system-level behaviors. Going beyond the ability for individually selected technologies, policies, people, products, services, information or processes to achieve *component*-level goals, the logic of emergence captures the importance of the interactions between such components on achieving *system*-level objectives. Another such systems-theory principle is *hierarchy*—and is directly related to the observed phenomena by which behaviors at a given level of complexity are irreducible to (and thus, inexplicable by) the behavior or design of its component parts. Here, hierarchy is a functional description for understanding, defining, and evaluating the characteristics that generate, separate, and connect these levels of complexity. Succinctly, the logic of hierarchy asserts that higher-ranking components (or influences) constrain the range of possible behaviors of components (or influences) at lower levels.

In addition, current efforts in systems engineering are focused on better conceptualizing how to coordinate these systems-theory principles for better understanding how interactions—both between components and with environmental influences—impact the ability of increasingly complex systems to achieve desired objectives. Addressing such interdependence in systems engineering includes identifying and designing for feedback, or how output from component A's interaction(s) with other components (or environmental influences) influences the next set of inputs back into component A actions. According to [6], as systems increase in complexity

> it is naïve to think that problem definitions and requirements will be isolated from shifts and pressures stemming from *highly dynamic and turbulent development and operational environments* (p. 38, emphasis added).

If this interdependence is true, then systems engineering provides a platform for better mitigating multidomain interdependencies between observed in treaty-based nuclear safeguards operations. Efforts to better engineer complex systems offers mechanisms by which to design nuclear facilities in such a way to account for socio-technical interdependencies observed in international safeguards by expanding design options to include non-traditional influences on system performance. By replacing the emphasis on component-level performance with a focus on system-level performance, systems engineering uses functional requirements as the scaffold for selecting, arranging and deploying interacting sets of components to achieve desire goals.

Recent Sandia research identified advantages from considering nuclear activities as complex systems to leverage emergence and hierarchy in evaluating safeguards (as well as safety and security) [7,8]—including benefits capable of matching the complexity expected with remote international or transboundary deployment environments or new fuel material characteristics.

SYSTEMS ENGINEERING FOR INTERNATIONAL SAFEGUARDS

At the 2022 *Topical Issues in Nuclear Installation Safety: Strengthening Safety of Evolutionary and Innovative Reactor Designs Meeting* hosted by the IAEA, some of the advantages of invoking a systems-engineering perspective for safeguards were introduced [8]. Albeit as part of an argument for enhancing safeguards-security-safety (3S) interactions, interpreting international safeguards through a systems-engineering lens aligns useful concepts and principles to anticipated A/SMR-related challenges. For example, consider describing international nuclear safeguards in terms of emergent behaviors. From this perspective, safeguards is *not just* ensuring the highest quality of nuclear material measurements, physical and electrical containment, electrical surveillance or environmental radiological signal monitoring—it becomes observed in the *interactions* between the interacting technological and procedural elements that compose these efforts. If international safeguards are an emergent property of A/SMRs, then the anticipated challenges become new design considerations for tomorrow's safeguards solutions.

Similarly, the concept of hierarchy provides another approach for designing and developing safeguards solutions. Characteristics of traditional nuclear facilities—including their larger and well-established infrastructure—can be perceived as hierarchical constraints on associated C/S capabilities. For A/SMRs, in turn, anticipated operational characteristics play a similar role and

Table 2. Comparison of potential A/SMR-related impacts on timeliness and verification safeguards objectives, where [+]/[-] designates an element of a reactor technology that enhances/challenges the timeliness and verification safeguards objectives.

	Nuclear material accounting [NMA]		**Containment & Surveillance [C/S]**		**Design information verification [DIV]**		**Environmental sampling [ES]**		**Complementary access [CA]**		**Open source [OS]**	
Goal(s) *[Timeliness & Verification]*	Provide material management and accounting, maintain continuity of knowledge		Establish physical integrity of an area or items and maintain continuity of knowledge of the area or items		Verify presence, location & purpose of all declared components of a facility		Verify declared activities at a facility		Verify that no undeclared activities are taking place		Verify that no undeclared activities are taking place, maintain understanding of a state's technical capability	
	Time	Verify	Time	Verify	Time	Verify	Time	Verify	Time	Verify	Time	Verify
Traditional NPPs	[+] Known fuel re-loading schedules [+] Lower enrichment	[+] Easier access to fuel	[+] Often have reliable connections for data transmissions	[+] More space & flexibility to apply C/S	[+] Reactor does not move from construction location	[+] More direct ways to test equipment & check transfer routes & hold up points	[+] Routine process for taking swipes for IAEA analysis	[+] Confirm known activities [+] Identify undeclared activities	[+] Simple logistics for inspections	[+] Staff size can support inspections	[+] Simple logistics for reviewing relevant reports	[+] Range of relevant reports exist
A/SMR	[-] Potential for online or continuous refueling [-] Higher enriched HALEU fresh fuel [-] Need for new measure techniques	[-] Reduced access to fuel for DA (for certain fuel types)	[-] Need for robust data transmission for "state of health" from remote locations (if physical inspection infrequent) [-] May require new seals for long life cores	[-] Need for more resilient container solutions (for remote or moveable options)	[-] Difficult to account for time between manufacture & installation	[-] May need to verify multiple times—e.g., at manufacturing & installation site	[-] Increased difficulty in executing sampling at remote locations	[-] Potential difficulty in protecting remote comms	[-] Expected remote deployment	[-] Potential small onsite staff presence	[-] Unknown existence of relevant reports	[-] Unknown existence of relevant reports

suggest that future C/S capabilities may need to navigate less robust transmission lines in remote locations, seals sufficient for long life cores or more resilient containment solutions. Leveraging the systems engineering perspective of incorporating interdependence is conceptually similar to popular calls for “safeguards-by-design” [9]. For example, many A/SMR designs are anticipated to have a greater reliance on bulk-accounting approaches if new nuclear materials are in pebble or liquid fuel form. In contrast to item-based, the inherent measurement uncertainty in bulk accounting techniques is potentially exacerbated by remote or transportable operations—a set of interdependencies that help identify where safeguards solutions should focus.

After combining the concepts of emergence, hierarchy and interdependence, the result is a notional systems-engineering-based framework for international safeguards aimed to mitigate a representative set of the previously described challenges. Ultimately, incorporating a systems-engineering perspective helps reconceptualize traditional nuclear safeguards goals as functional objectives. Rather than focusing solely on how current NMA or DIV technologies might need to be enhanced, a systems-engineering perspective would help identify what (if any) differences exist in meeting NMA and DIV timeliness and verification objectives for a given A/SMR.

Table 2 summarizes a representative set of A/SMR-related impacts on international safeguards in terms of timeliness and verification as functional requirements. Table 2 designates how reactor or facility characteristics may enhance [+] or challenge [-] safeguards solutions—where [-] items can be repurposed as engineering design considerations. What results are then sets of functional requirements that current and/or future technologies can be designed to achieve.

CONCLUSIONS & INSIGHTS

Systems engineering—as the art of manifesting a solution—provides several advantages for navigating A/SMR-related challenges to the international nuclear security regime. Invoking such concepts as emergence, hierarchy, interdependence and functional requirements yields a framework for transforming these challenges into design considerations to encourage desired levels of safeguards performance at A/SMR facilities. Despite the advertised benefits of A/SMRs, a systems-engineering approach is well positioned to support responsible operation of increasingly novel A/SMR facilities in increasingly complex operational environments. For example, effective safeguards solutions will manifest from better understanding interactions between new operational environments, novel material characteristics and safeguards objectives. Here, successful A/SMR deployment would also seemingly benefit from better characterizing how safeguards CA timeliness objectives may conflict with expected operational rhythms, as well as better identifying potential gaps in safeguards DIV verification objectives. Conversely, effective A/SMRs safeguards solutions can manifest by reinforcing NMA timeliness objectives in a way that leverages operational quality assurance procedures—suggesting opportunities for “force multipliers” for A/SMR safeguards.

Explicitly identifying—and designing for—emergence, hierarchy and interdependence offers a broader solution space within which to creatively increase the effectiveness of safeguards solutions for A/SMR designs. By using these concepts to generate functional requirements, A/SMR-related challenges can transform into systems-engineering design goals [6,7]. In addition, these systems engineering design goals provide the framework for trade-space analysis to trace the origins of negative interactions to either implementation, design, or requirements decisions. From this perspective, interdependencies between operational environments and CA or DIV functional needs translate into design decisions focused on improving system performance, reducing the risk of poor system performance or (ideally) a combination of the two. In an A/SMR context, safeguards design can be reframed in terms of designing NMA, DIV, ES, CA and OS solutions to reduce the possibility space for an undesired outcome or performance.

Though based on a representative set of considerations, the benefits of applying systems engineering to evaluating safeguards for A/SMRs suggests a need for continued exploration. Moreover, a "transdisciplinary and integrative approach…using…scientific, technological, and management methods" is well-suited for navigating A/SMR-related challenges to safeguards that trend toward overcoming novel fuel characteristics, new reactor systems and remote operational environments. Next steps could include (but not be limited to):

- Surveying current safeguards solutions from a systems-engineering perspective to describe safeguards goals/objectives as engineering functional requirements;
- Conducting more detailed investigations into applying general systems-engineering concepts to a range of A/SMR technologies and deployment combinations; and,
- Applying leading-edge systems-engineering analysis techniques (e.g., systems theoretic process analysis [10]) to A/SMR safeguards.

The IAEA is awash in data, and systems engineering provides a strong mechanism for digesting and reconciling multi-form, disparate information flows into determinations. In addition, the logical foundation of systems engineering seems well-suited to support the IAEA's call for state-level safeguards approaches based on structured and technical methods. Ultimately, lessons learned and insights gained from applying systems engineering can develop enhanced capabilities for all A/SMR stakeholders—potential vendors, operators, hosts and the IAEA—to efficiently and effectively meet international safeguards obligations.

REFERENCES

[1] Whitlock, J. and J. Sprinkle (2012) "Proliferation Resistance Considerations for Remote Small Modular Reactors," AECL Nuclear Review (invited article), 1(2), pg. 10-13.

[2] International Atomic Energy Agency (2022) "IAEA Safeguards Glossary (2022 Edition)," < https://www-pub.iaea.org/MTCD/publications/PDF/PUB2003_web.pdf>.

[3] Cloutier, R.J. and N. Hutchinson (eds) (2022) "Systems Engineering Body of Knowledge," <https://sebokwiki.org>.

[4] International Council on Systems Engineering (2023) "About Systems Engineering," <https://www.incose.org/about-systems-engineering>.

[5] Pyster, A., N. Hutchinson and D. Henry (2018) The Paradoxical Mindset of Systems Engineers, Wiley.

[6] Keating, C., R. Rogers, R. Unal, D. Dryer, A. Sousa-Perez, R. Safford, W. Peterson, and G. Rabadi (2003) "System of Systems Engineering," Engineering Management Journal 15(3), pg. 36-45.

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

[8] Williams, A.D., B.B. Cipiti, J.J. Bland, D.M. Osborn, A.S. Evans (2022) "Lessons Learned from Exploring Safety, Security, and Safeguards Interfaces in Advanced & Small Modular Reactor Technologies," IAEA Topical Issues in Nuclear Installation Safety: Strengthening Safety of Evolutionary & Innovative Reactors.

[9] Lee, J.S., J.Y. Doo, J. Whitlock (2021) "Safeguards by Design (SBD) for Small Modular Reactors (SMRs)," Proceedings of the Institute for Nuclear Materials Management.

[10] Leveson, N. (2012) Engineering a Safer World: Systems Thinking Applied to Safety, MIT Press.