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

ENHANCING A SYSTEMS ENGINEERING AND REGULATORY LIFECYCLE-BASED FRAMEWORK FOR SECURITY-BY-DESIGN

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

ABSTRACT

"By-design" is an increasingly popular phrase in the expanding discussions revolving around advanced and small modular reactors (A/SMR)—particularly in terms of achieving desired levels of nuclear security performance. A primary driver for these concepts relates to claims that earlier incorporation of such performance-based design decisions results in more efficient facility designs and less re-work. Current thinking to achieve "security-by-design" (SeBD) includes applying traditional physical protection design strategies "early in the design lifecycle," seeking "intrinsic security…as an integral part of the organization," and making "security…[a] part of the facility lifestyle." Yet, both internal and external dynamics related to A/SMRs suggest a need to recharacterize popular interpretations of security-by-design.

In response, Sandia National Laboratories—with support from the U.S. National Nuclear Security Administration's (NNSA) Office of International Nuclear Security (INS)—has introduced a model framework for SeBD that is based on systems engineering and the regulatory lifecycle. Invoking key concepts from systems theory, this framework describes SeBD options by aligning best practices in engineering design with best practices in regulatory decision-making. In contrast to retrofitting security solutions to already completed facility designs, this framework categorizes SeBD options based on whether the A/SMR facility designer (e.g., vendor), operator (e.g., utility), or designer (who plans to own and operate their own facility) should take primary responsibility for execution. As demonstrated in a set of notional use cases, this systems engineering and regulatory lifecycle based approach to SeBD can result in more economical design for, and efficient engineering of, security solutions for A/SMRs.

After briefly contextualizing the anticipated benefits of "by-design" concepts, this paper will summarize the range of popular interpretations—including the latest views on "security-by-design." This paper will then review the foundations and characteristics of a systems engineering and regulatory lifecycle framework for SeBD. Next, a set of representative use cases demonstrate the efficacy of this approach, as well as more precisely describe the related benefits. Lastly, this paper will discuss conclusions and insights for the adequacy of this systems engineering and regulatory lifecycle framework, as well as implications for next steps toward continued refinement and deployment.

* SAND2023-03477C, 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.

INTRODUCTION

"By-design" is an increasingly popular phrase in the expanding discussions revolving around advanced and small modular reactors (A/SMR)—particularly in terms of achieving desired levels of nuclear security performance. The postulated benefits across the range of A/SMRs—which include smaller operational footprints, greater deployment flexibility and inherently safe processes—introduce new considerations for ensuring adequate security performance. Such considerations include (but are not limited to) novel sources of operational uncertainty in A/SMRs, increasing complexity in anticipated operational environments and nascent (and evolving) regulatory practices.

Yet, these considerations also present an expanding opportunity space for exploring new mechanisms for ensuring adequate security performance at new nuclear facilities. For example, as design decisions are being made amidst evolving operational and regulatory realities, there is a space for considering security solutions at the same time. If desired security performance can be perceived as an emergent property, then it can also be described in terms of cost to address (or fix) problems and flaws. From this perspective, the "1:10:100 Rule" (Figure 1)—which is a heuristic used in technological product development and manufacturing to describe the relative advantage of fixing problems early—is a useful mental model for addressing security in A/SMR development. In short, this heuristic suggests that *the same* fix will cost $1 in the design/ requirements phase, $10 in the development phase, and $100 in the operational phase [1].

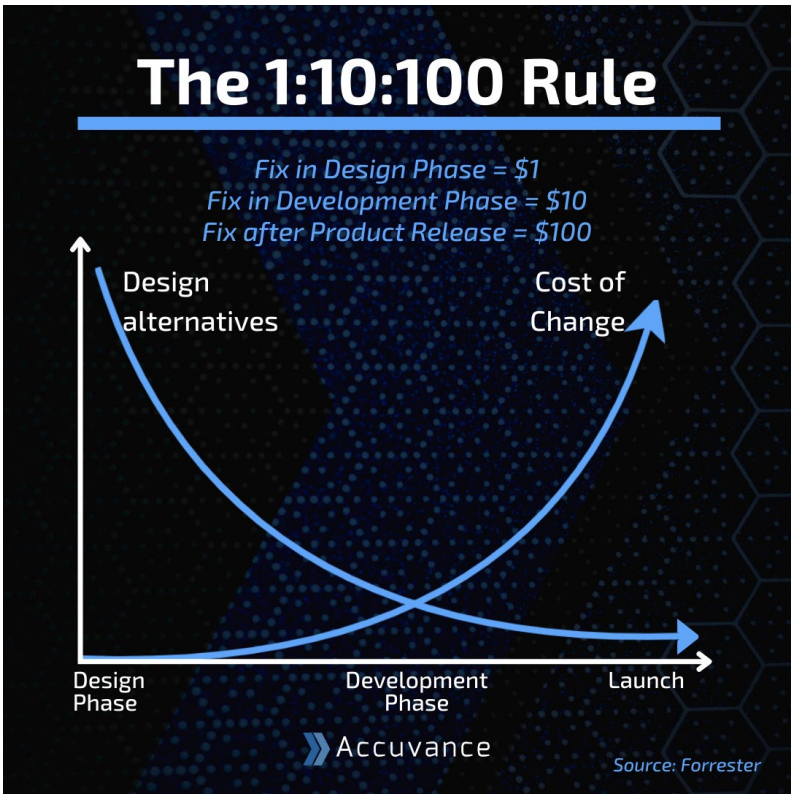

Figure 1. The 1:10:100 Mental Model [1]

Current thinking to achieve "security-by-design" (SeBD) includes approaches that advocate applying traditional physical protection design strategies "early in the design lifecycle," seeking "intrinsic security…as an integral part of the organization," and making "security…[a] part of the facility lifestyle" (Table 1). A primary driver for these concepts relates to claims that incorporating such performance-based design decisions earlier results in more efficient facility designs and less re-work. And while there are clear distinctions between the different interpretations of SeBD presented in Table 1, the common spirit across the definitions is identifying and exploiting opportunities to take security credit for design-related decisions throughout the facility's development lifecycle.

Table 1. Summary of Interpretations for Security-by-Design (SeBD), adapted from [2]

Author	**Interpretation of SeBD**	**Primary Advantages**
Sandia National Laboratories & Japanese Atomic Energy Agency (JAEA) [3]	"early in the design process, consider the facility mission…[to] make security response…easier" or "based on operations, processes, and plant layout, determine equipment requirements for physical protection."	• Security systems can be designed *before* the facility is constructed • Early effectiveness evaluation (ideally) may lead to reduced costs
World Institute for Nuclear Security (WINS) [4]	"intrinsic security…as an integral part of the organization…to provide a security margin proportionate to the risk without excessive disruption of business"	• Focus on organizational & operational issues for commercial facilities • Leverages *Crime Prevention Through Environmental Design* approach
Canadian Nuclear Safety Commission (CNSC) [5]	"integration of security at the earliest stages to mitigate malicious acts, and [SeBD] should be part of the facility lifecycle"	• Shift from prescriptive to performance-based regulations

Starting with the anticipated increase in security performance and cost effectiveness, key elements of systems theory can help recharacterize these popular interpretations of SeBD. More specifically, systems theory provides the basis for articulating an engineering process that incorporates core elements of desired security behavior into intrinsic considerations or features of facility level design. Such a recharacterization has the potential to support three broad benefits for SeBD. First, such an approach can provide additional clarity—and possible stakeholder consensus—for identifying how to gain security performance improvements and cost reduction. Second, such an approach can aid in aligning—and anticipating—key design decisions that impact meeting security-related regulatory requirements. Third, such an approach is flexible enough to provide security insights for scenarios in which an A/SMR vendor may need to engage multiple competent security authorities, multiple licensing processes, or various regulatory requirements.

FOUNDATIONS & CHARACTERISTICS FOR A NEW APPROACH TO SeBD

Lifecycle models are commonly used to assess and visualize interactions of emergent behaviors for complex systems—and are uniquely positioned to illustrate SeBD. For example, engineering lifecycle models describe how decisions related to manifesting desired behaviors of systems change in scale and scope as the design matures. Such lifecycle models are useful for mapping different levels of system maturity with associated levels of uncertainty to help illustrate cost-

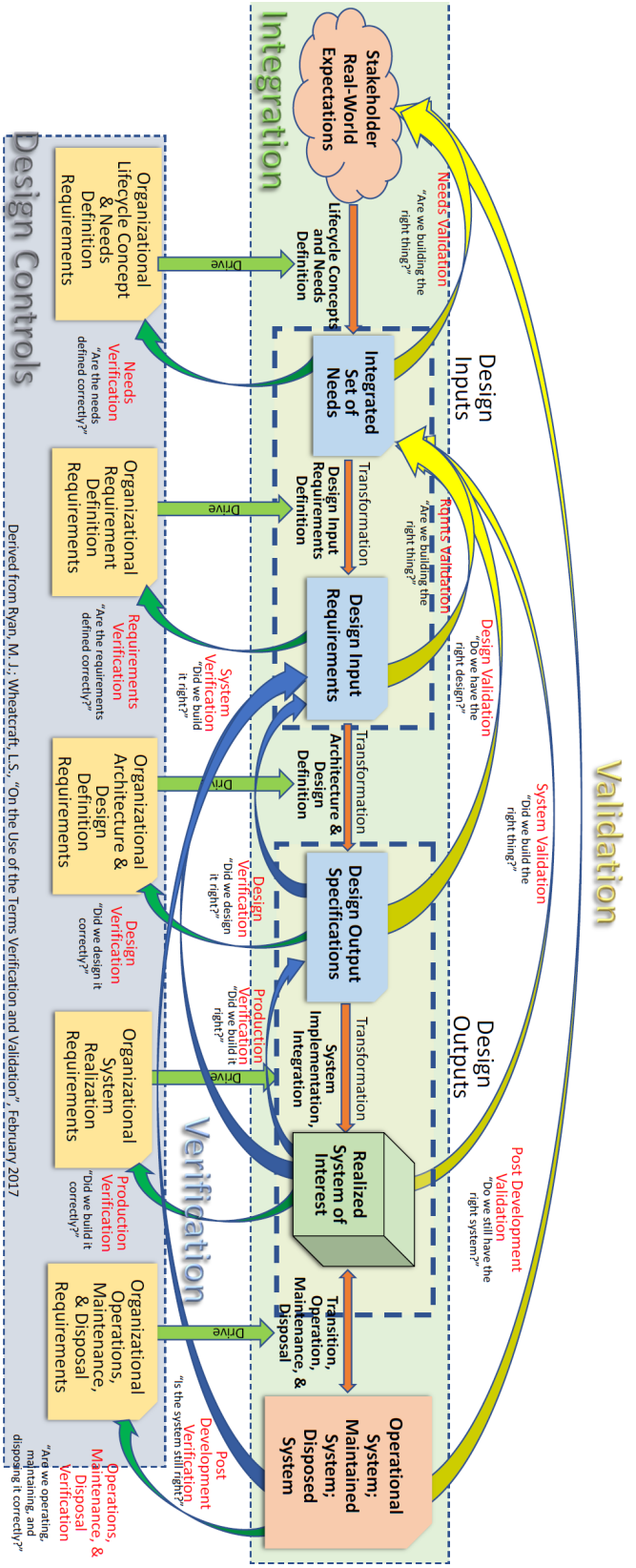

Figure 2. A systems validation and verification systems model as an example of a joint engineering and regulatory lifecycle model [8]

versus-performance tradeoffs from conception to deployment. This process is further enhanced by leveraging the series of internal reviews (e.g., preliminary or interim design reviews) as active feedback and regular opportunities to incorporate desired performance objectives—like security—early, frequently, and continuously. Such engineering lifecycle models also provide increased clarity in communicating how the security equities of multiple stakeholders are addressed.

Consider, for example, the generic engineering lifecycle provided by the International Council on Systems Engineering (INCOSE), which identifies a set of "typical decision gates," including: new initiative approval, concept approval, development approval, production approval, operational approval, and deactivation approval [6]. If the tradition is to introduce security elements between the "production approval" and "operational approval" decisions gates, then SeBD involves incorporating them between the "new initiative approval" and "development approval" decision gates. From this perspective, engineering lifecycle models provide a strong technical foundation to guide trade-off discussions on the early inclusion of security elements.

Lifecycle models have similarly been used to increase clarity in understanding license and regulatory requirements. For example, such models can either help identify where performance requirements might be standardized, highlight where exceptions might be necessary, illustrate issues that might hinder (or accelerate) regulatory development, or mitigate issues related to regulatory capture (a phenomenon occurring in later lifecycle stages, where the independent regulatory body is (in)directly controlled by the industry it was created to oversee). One generic lifecycle model is built on seven stages of regulatory development: gestation, infancy, childhood, youth, maturity, old-age, and death [7]. Similar to engineering lifecycle models, regulatory, and licensing lifecycle models provide a structured mechanism for understanding how "initial regulatory arrangements will undergo a large number of changes prior to maturity as the regime gradually becomes more or less locked-in…[and] standard[ized] [7]."

Both engineering system and regulatory lifecycle models are useful for enhancing transparency and opportunities for SeBD. Consider Figure 1 as one example of how engineering and regulatory lifecycle models can be combined. As shown, this model offers a framework that clearly identifies where technical decisions made toward desired performance of the system (culminating in the "realized system of interest") aligns with various types of requirements (in the "design controls" section [8]). In Figure 1, validation refers to the extent to which a given stage of system development meets desired performance expectations, and verification refers to the extent to which stated requirements adequately capture the needs of system performance.

Earlier in the process, while the system is not close to being fully realized, there is a higher degree of flexibility in updating the requirements to better match expected system behaviors. As the system becomes more fully realized (moving to the right in Figure 1), opportunities to change the requirements are reduced, and the focus transitions to making design decision *within the constraints* of the requirements. Further, the relationship between progress on system realization and requirements maturation is a series of feedback loops that enable an ongoing conversation on

how best to ensure that the requirements categorizing and the design decisions manifesting the system at each realized state are meeting the desired behaviors.

Applying such a combined lifecycle approach provides a framework to explore how to optimize the complex—and often complicated—security performance-cost-licensing trade space between A/SMR design and operations stakeholders. This joint engineering-and-regulatory lifecycle framing is helpful for delineating security-related responsibilities between vendors (A/SMR reactor designers and manufacturers) and utilities (A/SMR facility owners and operators). Here, the vendor is responsible for the initial reactor and facility design with the goal of receiving a certified design that could be sold to a utility. The utility, on the other hand, is responsible for actualizing a certified design through operations and maintenance of the reactor and facility (through decommissioning) over its lifecycle. In terms of Figure 1, the A/SMR vendor is primarily responsible for activities up through "design output specifications," and the utility is responsible for the activities under "realized system of interest" and "operational-maintained-disposed system."

In the context of the performance requirements established by the U.S. Nuclear Regulatory Commission (NRC), potential A/SMR vendors are seeking an approved design certification application (DCA), and utilities are seeking an approved combined operating license[1] (COL) to construct and operate a nuclear facility. This approach helps frame different areas in which vendors and utilities can pursue SeBD and take security "credit" for safety and facility design decisions made toward either DCA or COL approval. Simply stated, a regulatory and engineering lifecycle model approach offers two pathways of SeBD. The first is based on the extent to which security requirements for the COL can be addressed in the DCA phase by claiming "security credit" for safety and operations-related facility design decisions. The second pathway is based on the extent to which security regulations for the COL can be addressed during pre-deployment stages of the lifecycle.

Consider Figure 3 as a way to compare the conceptual benefits of these two SeBD pathways with traditional security design approaches. Observations suggest a strict separation of security-related responsibilities between designer and operator, which have resulted in security being addressed *after* major reactor and facility design decisions are made. In other words, security requirements are highly rigid—serving primarily as constraints—and are addressed as retro-fitted security solutions to the COL-approved facility design. In this scenario—illustrated by the green lines labeled "Baseline: Traditional retrofit approach to security" on the right side of Figure 2—an overwhelming majority of security costs are assumed by the operator. Likewise, the two SeBD pathways showcase where and how security could be considered earlier in the facility's lifecycle—both before completing (the purple lines in Figure 3) and soon after completion of the DCA (the red lines in Figure 3).

The extent to which this two-pronged SeBD pathway manifests in "security credit" successfully claimed closer to (or within) the DCA suggests two interesting outcomes. First, costs related to

[1] For clarity in explaining this new proposed approach, this paper assumes utilities will seek a "combined operating license," despite the alternate process of seeking separate construction and operating licenses.

retrofitting security solutions to post-COL designs can be reduced—if not eliminated. This reduction has the potential also to drive down overall operator-specific costs of meeting security-related requirements for the COL. For illustration, the sizes of the teal and orange triangles on the left side of Figure 3 represent the cost sharing/savings from this proposed two-pronged SeBD pathway. Second, as shown by the purple lines in Figure 3, some of the security costs can be assumed by the designer. This transfer indicates that "security credit" can be claimed for pre-DCA safety and operations-related design decisions, which helps reduce overall security cost. The framework allows for additional nuance, as illustrated in the two purple lines on the DCA side of the figure, which represent two different strategies. One strategy seeks "security credit" in the initial facility design decisions, while the other seeks it in the design certification application.

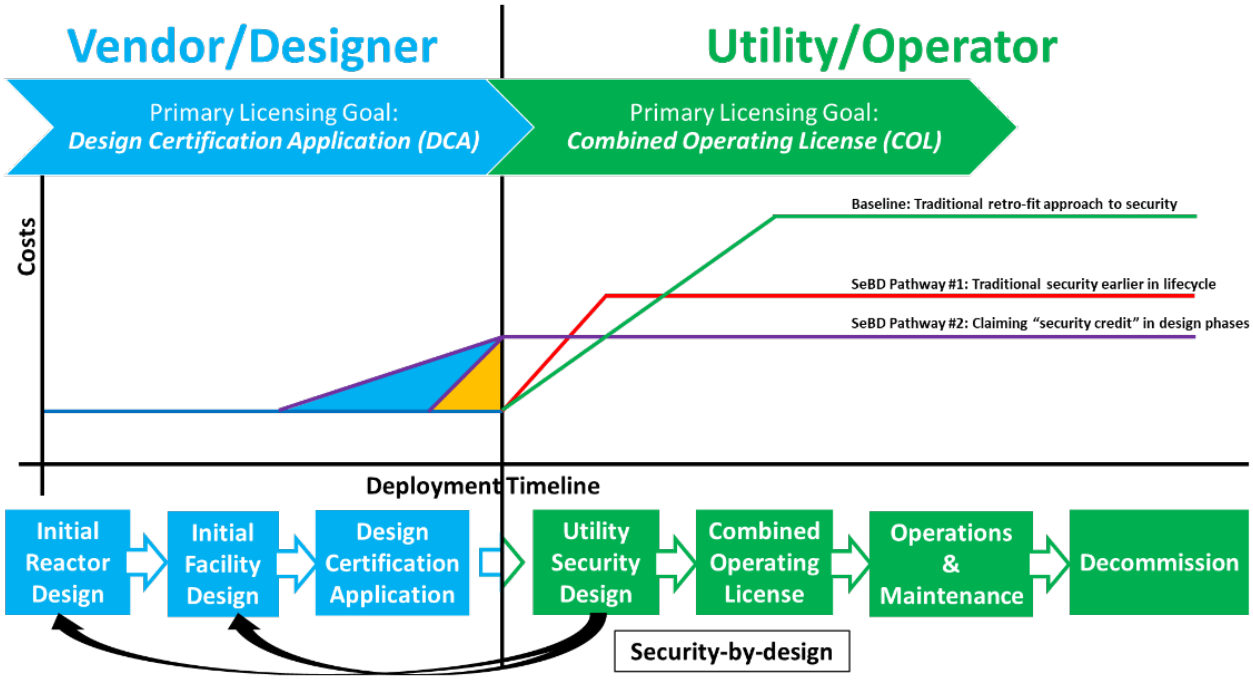

Figure 3. Comparing traditional security approaches to the proposed SeBD approach using a regulatory/engineering lifecycle model, recreated from [2]

A NEW APPROACH TO SeBD: DEMONSTRATION CASES

U.S. Case: As A/SMR vendors continue down their respective licensing pathways, they will provide additional opportunities to demonstrate this proposed regulatory and engineering lifecycle approach. For example, consider the following description taken from NuScale's DCA:

> The NuScale Power design provides the design descriptions for engineered [physical security system] PSS and credited design features (e.g., structural walls, floors, and ceilings, and configurations of the nuclear island and structures); descriptions of intended security functions and performance requirements; design bases for the detailed design; and supporting technical bases that a

> COL applicant will incorporate by reference as part of its design and licensing bases [9, p. 13.6-1].

There are two interesting elements in this description. First, "credited design features" such as physical infrastructure and physical layout are hinted as helping meet security requirements. Second, "descriptions of intended security functions" are provided to aid a future COL application—suggesting the shift away from traditional models of retrofitting security.

Canadian Case: The Canadian Nuclear Safety Commission (CNSC) is the nuclear regulatory authority of the Canadian government. The CNSC incorporates 19 focus areas into its Phase 1 and Phase 2 applications for new nuclear facilities. The 19 focus areas include many areas where SeBD could be integrated to inherently increase the security of new nuclear facilities to include A/SMR. For example, consider the first focus area, which includes descriptions of plant operations, defence-in-depth, safety goals and objectives, and dose acceptance criteria. Similar to Figure 2, where this first focus area introduces plant layouts and site descriptions into the licensing process, so to can early discussions on physical protection systems (which are tightly coupled to plant configuration).

One specific example is illustrated in ensuring there is enough standoff distance and protection provided to vital (or other critical) areas for protection against large vehicle-borne explosive devices. Even early in the process, the facility design should consider the maximum allowable vehicle-borne explosive device weight and capabilities (typically defined in a threat assessment, like a design basis threat [DBT]). As a potential DCA under the CNSC moves from Phase 1 to Phase 2, increasingly detailed blast analysis simulations (e.g., shock physics codes) could be executed to estimate the survivability of different proposed structure designs. As the design moves closer to an approved DCA, the potential benefits of the different SeBD pathways in Figure 2 may decrease. Yet, this proposed engineering and regulatory lifecycle model helps navigate the cost-security-performance tradespace between using building materials, plant design, standoff distance, or extra ballistic shielding to protect vital areas from such explosions in this example.

Based on the engineering and regulatory lifecycle model, A/SMR vendors applying for licenses to operate in Canada should consider developing security concepts into the site design and layout to take advantage of SeBD benefits. This proposal allows the CNSC and the operator to engage in the regulatory process at Phase 1 and ensure that security is integrated into the entire lifetime of the plant.

Multiple Country Deployment of the same A/SMR Technology Case: For this example, assume an A/SMR vendor wants to deploy in Canada and the U.S. Doing so would require the vendor to consider *both* the 19 focus areas in the CNSC license application process and the license application for the U.S. NRC. In this scenario, this engineering and regulatory lifecycle model can help the A/SMR vendor to identify potential areas of overlap between CNSC and U.S. NRC licensing applications. For example, an A/SMR vendor would need to identify the security boundaries in both applications. Invoking the feedback relationship described between facility design status and regulatory requirements, decisions on the size and orientation of the Limited Access Area (aka Owner Controlled Area), the Protected Area (PA), and Vital Areas (VAs).

Similarly, this model could be used to evaluate the relative effectiveness of facility design decisions made in one country on the anticipated security performance in the other.

Whether identifying options to achieve adequate standoff performance for VBIEDs or the security boundaries to ensure the survivability of structures, systems, and components, this proposed model provides an illustrative framework. The A/SMR vendor can then apply lessons from these analytical results in its license applications to both countries. Such information could also increase the marketability of A/SMRs by using the engineering and regulatory lifecycle model to illustrate the potential benefits more clearly (e.g., the size and location of the orange and purple triangles in Figure 2).

CONCLUSIONS & IMPLICATIONS

Where the driving factors behind developing this proposed regulatory and engineering lifecycle model approach stem from professional observations and experiences, the two related pathways of SeBD also offer several implications for meeting both domestic international nuclear security regulations more cost effectively.

The first pathway is consistent interpretations for incorporating traditional security elements earlier in the lifecycle. As such, there is a straightforward opportunity to incorporate this element of SeBD into international dialogues by mapping technical best practices for nuclear security (e.g., IAEA's Nuclear Security Series No. 13) with recommended regulatory processes outlined for new nuclear projects (e.g., IAEA's Nuclear Energy Series No. NG-G-3.1). A few examples here include addressing plant layouts to create choke points on anticipated adversary paths before the DCA, evaluating building designs capable of advanced technology deployment (i.e., hallway and ceiling dimensions that allow for remote operated weapon system deployments) during the DCA, and defining wall thickness and reinforced doors placement after the DCA.

Codifying the second SeBD pathway into international best practices might be a little trickier but will likely happen as the expected financial benefits are realized. Examples here include laying extra conduit around the nuclear island to ease future deployment of new technologies (COL) or using modeling and simulation capabilities to inform plant design and configuration in each design (DCA) stage of the facility to develop effective security systems that adapt with each facility design change.

A/SMR vendors should also consider using the proposed SeBD approach throughout the entire lifecycle of their facilities. Revisiting SeBD in general—and this engineering and regulatory lifecycle model specifically—increases the potential for coordination with additional utilities that are interested in the reactor technology, especially under different use cases. For example, if the utility and the vendor agree that spent fuel will be stored onsite, then future license applications will be impacted. Yet, this SeBD model provides a rigorous, structured, and iterative mechanism for exploring various security solutions or adapting to the impacts of onsite spent fuel storage on site layout and plant operations. More specifically, in some countries new security areas and site layouts for the spent fuel may be required in the initial license application for the facility.

Similarly, as A/SMRs are being considered for a wider range of uses (including district heating, process heating, or desalination) new deployment locations, operating environments, and plant layouts create both challenges to—and opportunities for—effective nuclear security. The proposed SeBD model is flexible enough to help ensure protection of any intended function associated with an A/SMR. Consider, for example countries who may be relying on the electricity production as a central measure in their energy mix. Therefore, A/SMR vendors may be asked to extend their security solutions to non-typical nuclear security areas. These requests may include, for example, the desire to protect switchyards being fed by electricity generated by the A/SMR. The proposed engineering and regulatory lifecycle based SeMD model affords the chance to compare different protection strategies. In a traditional strategy, the switchyard is given its own retro-fitted security solution. In contrast, the SeBD approach allows for considering putting the switchyards inside the protected area before, during, or (perhaps shortly) after a DCA is approved. Here, protection benefits are extended to switchyards in a manner that improves overall site security performance and is likely more cost-efficient.

By highlighting the trade-offs for addressing security requirements at different points in the lifecycle, this engineering and regulatory lifecycle model provides three key benefits. First, it offers a rigorous and structured approach to identify—and even optimize—SeBD decisions. Second, it provides pathways to introducing security earlier, more frequently, and continuously in A/SMR development. Lastly, it provides a common model to help encourage consensus and transparency in the financial and performance benefits of SeBD across the vendor, utility, regulatory, and nuclear security stakeholders.

REFERENCES

[1] Accuvance (2022) “The 1”10”100 Rule), < https://accuvance.com.au/accuvance-the-110100-rule/>

[2] Williams, A.D. and A.S. Evans (2022) “A LICENSING & ENGINEERING SECURITY-BY-DESIGN MODEL FOR ADVANCED & SMALL MODULAR REACTORS,” Proceedings of the Annual Meeting of the Institute of Nuclear Materials Management (virtual).

[3] Snell, M.K., et.al (2013) “Security-by-Design Handbook,” SAND2013-0038, Sandia National Laboratories, Albuquerque, NM.

[4] World Institute for Nuclear Security (2019) “Implementing Security by Design at Nuclear Facilities,” WINS International Best Practice Guide, Vienna.

[5] Duguay, R. (2020) “Small Modular Reactors and Advanced Reactor Security: Regulatory Perspectives on Integrating Physical and Cyber Security by Design to Protect Against Malicious Acts and Evolving Threats,” *International Journal of Nuclear Security*, 7(1).

[6] International Council on Systems Engineering (2021) “System Life Cycle Process Models: Vee,” Systems Engineering Body of Knowledge, <https://www.sebokwiki.org/wiki/System_ Life_Cycle_Process_Models:_Vee>, accessed Feb. 7, 2022.

[7] Newman, J. and M. Howlett (2014) “Regulation and time: temporal patterns in regulatory development,” *International Review of Administrative Sciences*, 80, pp. 493-511.

[8] Wilson, B (2022) “RWG Exchange Café: System of Systems (SoS) Guide Kick Off,” Online Event (recorded), International Council on Systems Engineering, <https://www.youtube.com/watch?v=FsDVci-zl2s>.

[9] NuScale, (2017) “Design Certification Application: Chapter 13—Conduct of Operations,” <https://www.nrc.gov/docs/ML1918/ML19182A241.pdf> accessed on Feb, 7, 2022.