SAND2022-8807C

Proceedings of the INMM Joint Virtual Annual Meeting
July 24-28, 2022

A LICENSING & ENGINEERING SECURITY-BY-DESIGN MODEL FOR ADVANCED & SMALL MODULAR REACTORS

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

Katherine Holt
Office of International Nuclear Security
National Nuclear Security Administration, DC, USA, katherine.holt@nnsa.doe.gov

ABSTRACT

Security-by-Design (SeBD) is a concept that has been garnering increased attention in professional discussions and gaining traction in commercial dialogues—particularly in support of increasing popularity of advanced and small reactor (A/SMR) technologies. The efficacy of SeBD faces a range of challenges, including (but not limited to) increasing complexity in anticipated operating environments for new nuclear facilities, non-traditional internal sources of uncertainty (e.g., new safety protocols for advanced reactors), developing standards on acceptable performance, and next generation security threats (e.g. unmanned aerial systems(UAS)). Yet, there remains a prevailing believe that SeBD can conceptually address these challenges, reduce associated costs, and enhance security performance.

Current research for the Advanced Reactor Security Program (ARSP) for the National Nuclear Security Administration's Office of International Nuclear Security (NNSA/INS)—supported by Sandia National Laboratories—is addressing the SeBD challenge. More specifically, ARSP is leveraging the experienced professionals of INS's nuclear security work around the world and current engagement with industry partners to develop a coherent approach to SeBD. Invoking elements of generic engineering lifecycle models, licensing lifecycle models, and complex systems analysis, ARSP has developed an SeBD model for A/SMRs. By employing the clarity and consensus provided by lifecycle models, a common understanding of the benefits and opportunities for SeBD becomes available for A/SMR stakeholders. Such an SeBD model also provides the foundation for discussions on optimizing security designs and decisions across the A/SMR performance, cost, and licensing tradespace.

After introducing the range of current approaches and discussing related gaps, this paper introduces key elements of lifecycle models, licensing lifecycle models, and complex systems analysis necessary to develop a more robust SeBD model for A/SMRs. Next, this paper discusses the logical foundation for the resulting lifecycle-based SeBD model, including a preliminary

* SAND2022-Programmatic Review, 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.

mapping against the current state of A/SMR licensing requirements and a set of representative examples of SeBD opportunities. Lastly, this paper will discuss key insights, representative implications, and summarize potential next steps for developing—and deploying—this lifecycle model of SeBD.

INTRODUCTION

The range of proposed advanced and small modular reactors (A/SMR) suggest a need to modify and enhance traditional approaches to protecting nuclear materials, operations, and facilities. While novel A/SMR designs advertise such benefits as greater deployment flexibility and smaller operational footprints, these capabilities also introduce additional considerations for ensuring adequate security performance[1]. In addition to the challenges offered by evolution/adaptation of traditional adversary threats (e.g., increased digital manipulation or unmanned aerial system [UAS] capabilities), other challenges can include

- increasing complexity in anticipated operating environments;
- non-traditional internal sources of operational uncertainty (e.g., new safety protocols for A/SMRs);
- nascent processes for developing standards for acceptable performance; and,
- changing regulatory and recommendation processes (e.g., U.S. Nuclear Regulatory Commission [NRC] regulations or International Atomic Energy Agency [IAEA] best practices documentation).

Yet, these challenges also present an expanding opportunity for exploring the concept of "security-by-design" (SeBD). Invoking key elements of systems engineering, a framework based on this SeBD definition can align—and anticipate—key design decisions that impact meeting security-related regulatory requirements. If successful, such a framing would help more clearly identify how to gain performance enhancement and/or cost reduction with SeBD for A/SMR facilities

BACKGROUND & CONTEXT

Borrowing logic from other "by-design" approaches to address elements of risk unique to nuclear facilities (including "safety-by-design" [2] and "safeguards-by-design" [3]), SeBD conceptually argues that adequate security performance is achievable more efficiently and economically when security operations are introduced *earlier* in the facility lifecycle. More recently, various interpretations of SeBD have been used as a catch-all term to describe (assumed) benefits of involving security thinking earlier in the nuclear facility design and development process (Table 1).

Leveraging one common feature across these interpretations—the anticipated enhancement of security performance and cost effectiveness—this paper proposes a new interpretation for an engineering process that incorporates core elements of desired security behavior into intrinsic considerations and/or features of facility level design. Invoking systems theory, this paper builds a SeBD framework that invokes elements of generic engineering lifecycle models, licensing lifecycle models, and complex systems analysis. Such a framework provides additional clarity—

and, resultant opportunities for consensus among stakeholders—provided by lifecycle models that supports a common platform for SeBD.

Table 1. Summary of Interpretations for Security-by-Design (SeBD)

Author	Interpretation of SeBD	Primary Advantages
Sandia National Laboratories & Japanese Atomic Energy Agency (JAEA) [7]	"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) [9]	"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) [10]	"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

LIFECYCLE MODELS TO SUPPORT SECURITY-BY-DESIGN

Lifecycle models are commonly used to assess and visualize interactions of emergent behaviors for complex systems. Engineering lifecycle models extend the ability for—and identify additional opportunities to—"engineer" different elements of desired performance and evaluate cost/performance tradeoffs across design/development/deployment processes. Engineering lifecycle models are useful for aligning different decision points with different levels of system maturity (and associated levels of uncertainty). For most engineering projects, the phases within lifecycles models are distinguished by a series of design reviews that support iterating from a conceptual design through a developed solution until uncertainty is minimized in a deployed system.

This process is further enhanced by leveraging this series of internal reviews as active feedback on anticipated performance of the design or developing solution—providing regular opportunities to incorporate desired performance objectives early and frequently into the design/development/ deployment process. An additional benefit of engineering lifecycle models is that they provide clarity to help multiple stakeholders better understand where their specific equities are addressed and how the overall system or solution is intended to operate (including across *other* stakeholder equities). In this manner, engineering lifecycle models are applicable to discussions around SeBD for AR and SMR facilities.

Consider Figure 1, referenced by the International Council on Systems Engineering (INCOSE), that compares lifecycle models across a range of complex systems disciplines. This matrix compares engineering lifecycle models used by a range of stakeholders, including both governmental and commercial entities. Reviewing these lifecycle models reveals high-level consistency in overall design/development/deployment structures. In Figure 1, this consistency is

simplified in the set of "typical decision gates" located at the bottom of the figure. These decision gates also provide opportunities to incorporate SeBD—including both identifying where in the design/development/deployment process security requirements can be discussed and the trade-offs related to incorporating elements of security at each point. For example, consider the tradition of involving security elements between the "production approval" and "operational approval" decisions gates.

Doing so allows security to be tailored to specific system designs, but also likely requires costly retrofits to the core system. In contrast, consider the possibility of incorporating elements of security in the design package in support of the "new initiative approval" decision gate. Doing so clearly counters the tradition of security as an "add-on," but also runs the risk of increasing the difficulty of converging on a coherent design of the core system itself. In this manner, engineering lifecycle models provide a strong foundation to support rigorous, technical discussions on the trade-offs related to incorporating elements of security across design, development and deployment processes.

Lifecycle models can also enhance overall management of designing, developing and deploying complex systems. For example, such models can increase clarity of license and regulatory discussions by aligning mandated requirements with ongoing technical reviews. Such additional clarity can produce a range of design, development and deployment benefits for engineered solutions. First, lifecycle models can help identify where performance requirements might be standardized across a particular industry or intended used. Second, lifecycle models can highlight where exceptions might be necessary, help support their justification, and anticipate future needs for similar exceptions. Third, regulatory lifecycle models can better illustrate elements that might hinder or accelerate the transition of the engineered solution through regulatory development. Lastly, such a lifecycle approach can help mitigate issues related to regulatory capture—where the independent regulatory body is (in)directly controlled by the industry it was created to oversee—which typically occurs in later lifecycle stages.

One categorization of licensing and regulatory lifecycle models is shown in Figure 2 (below), showing seven generic stages of regulatory development [12]. This lifecycle model describes regulations beginning at the point when a problem is recognized by stakeholders and met with nothing more than initial advocacy efforts. This "gestation" stage is followed by the "infancy" and "childhood" stages in which the new problem is mapped against current statutes and a desire for new rules increases. From this process of clarifying regulatory needs, the "youth" stage often sees an independent regulatory agency granted with rule-making authority. As the regulatory agency gains experience and establishes rules, the lifecycle model enters the "maturity" stage where ideologies and logical arguments are cemented and functionality becomes normalized. The "old age" stage follows, marked by long-standing regulatory understanding and procedures—and an increased potential for regulatory capture to emerge. Though not always experienced, taking the lifecycle model to its logical conclusion, the "death" stage consists of significant re-examination/re-creation or retirement of a regulation.

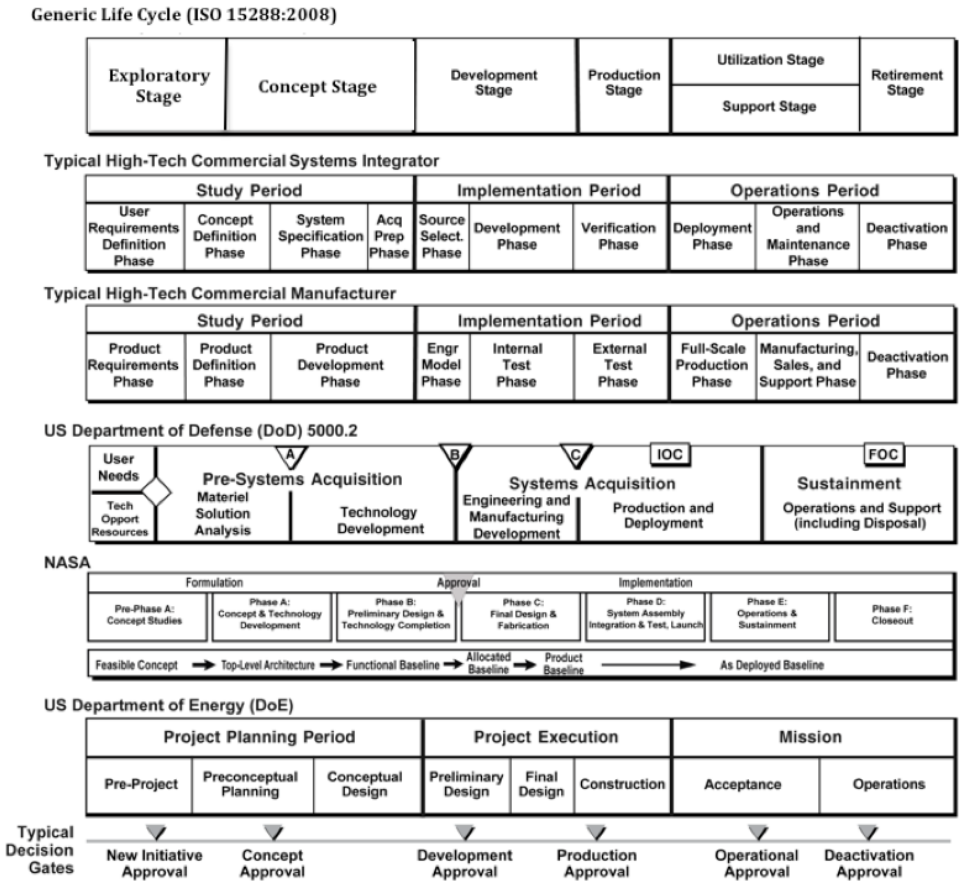

Figure 1. Comparison of generic engineering lifecycle models [11]

The lifecycle model provided in Figure 2 provides 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] [12]." Similar to engineering lifecycle models, there is not an assumption of automatic linearity through these stages. More specifically, each stage of the regulatory lifecycle model may take different lengths of time to complete and may even reverse itself (e.g., deregulation). This model *also* offers the benefit of capturing exogenous factors that can accelerate or hinder regulatory development—for example:

> …especially in areas of risk regulation, it is therefore plausible that for a regulatory regime to emerge, a *hazard must not only be identified* as a policy problem but must also have *tangibly manifested itself* in the form of a public crisis or emergency, in order to force the hand of decision makers. [12] (emphasis added)

Both engineering system and regulatory lifecycle models are useful for enhancing transparency and opportunities for SeBD, particularly considering the challenges observed with AR/SMR design, development and deployment.

Life-cycle stage	Issues	Task	Administrative techniques
I. Gestation	Emergence of problem on the agenda as a threat, hazard or risk	Recognizing that the issue has emerged	Public acknowledgement of issue
II. Infancy	Poor knowledge base; Attempt to adapt existing statutes and rules to current problems	Efforts at issue suppression; Stigmatization	Delay; Adaptive experimentation; Exhortation to encourage voluntary activity
III. Childhood	Desire to create new rules but no clear knowledge of what these rules/standards should be; Lobbying; Venue shopping	Standard-seeking; Large-scale research programs for hazard characterization; Initial quantitative risk assessments	Using principles rather than standards; Creation of an autonomous regulatory body
IV. Youth	Completion of hazards assessment; Development of standards; Frozen issue frames; Issue ownership by specific groups; Legal actions	Smaller-scale, maintenance research; Court activities	Emergence of more direct, authoritative state regulation; Rule adjustment; Litigation
V. Maturity	Normalization of the regulatory issues	Administrative activity	Emergence of specific agencies that 'own' the regulatory area
VI. Old Age	Regulatory capture; Emergence of clientelism	Maintaining a favorable environment for the regulatees	Self-regulation
VII. Death	Modification/death of the issue	Re-examining the issue and priorities	De/re-regulation

Adapted from: Bernstein, 1955; Howlett and Migone, 2012; Leiss, 2001; Otway and Ravetz, 1984.

Figure 2. Regulatory lifecycle model [12]

A REGULATORY & ENGINEERING LIFECYCLE MODEL APPROACH TO SeBD

For this perspective, if lifecycle models provide additional clarity for and understanding of regulatory needs, then they can also be used to enhance the ability of designs to meet those same regulatory needs. As a result, this paper proposes using a combined engineering and licensing lifecycle model to align—and anticipate—key design decisions that impact meeting security-related regulatory requirements. Such framing would help more clearly identify how to gain performance enhancement and/or cost reduction by addressing key "downstream" security licensing issues earlier in the engineering lifecycle. Combining these lifecycle approaches provides a framework to explore how to optimize the complex—and often complicated—security performance/cost/licensing trade space between AR and SMR design and operations stakeholders.

For AR and SMRs, consider the joint engineering and regulatory lifecycle framing provided in Figure 3, which shows a clear delineation in responsibilities between vendors (A/SMR reactor designers and/or manufacturers) and utilities (A/SMR facility owners and/or operators). In this framework, the vendor is responsible for the initial reactor and facility design for the goal of receiving an approved design certification application (DCA) from the NRC. Conversely, the utility is responsible for the operations and maintenance of the reactor and facility (through decommissioning) once they receive a successful combined operating license (COL). The DCA heavily focuses on meeting safety standards with minimal security considerations, while the COL encompasses nearly all the formal security requirements.

According to Figure 3, "security-by-design" evokes different conceptions for the DCA and COL portions of the lifecycle. More clearly, SeBD thinking during the DCA portion should focus on how a design can take security "credit" for safety and facility design characteristics. SeBD for the COL portion of the lifecycle should focus on addressing as many of the related security requirements in the design (pre-deployment) stages as possible. Simply stated, a regulatory and engineering lifecycle model approach offers two pathways of SeBD:

- 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 extent to which security regulations for the COL can be addressed during pre-deployment stages of the lifecycle

For clarity, consider how traditional security design approaches are driven by a strict separation of security-related responsibilities between designer and operator. Tradition has shown that the result is security being addressed *after* major reactor and facility design decisions are made. In other words, security requirements and regulations are addressed as the COL-approved facility design is retrofitted with security solutions. This is represented by the green lines labeled "Baseline: Traditional retrofit approach to security" on the right side of Figure 3 that shows how an overwhelming majority of security costs are assumed by the operator.

In contrast, the proposed regulatory and engineering lifecycle model approach to SeBD helps identify where and how security could be considered earlier in the facility's lifecycle—both before completing (the purple lines in Figure 5) and soon after completion of the DCA (the red lines in Figure 5). If this two-pronged pathway of SeBD manifest to justify "security credit" in/closer to the DCA, then two interesting outcomes occur. First, costs related to retrofitting security solutions to post-COL designs are reduced—if not eliminated—driving down the *both* overall security costs and operator-specific costs of meeting security-related requirements for the COL. For illustration, the size of the teal and orange triangles on the left side of Figure 3 represent the cost sharing/savings from this proposed regulatory and engineering lifecycle model approach, with the impact derived from the two-pronged SeBD pathway.

Second, some of the security costs can be assumed by the designer. As shown by the purple lines in Figure 3, claiming "security credit" for pre-DCA safety and operations-related design decisions can help reduce overall security cost. More specifically, the two purple line on the

DCA side of the figure 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.

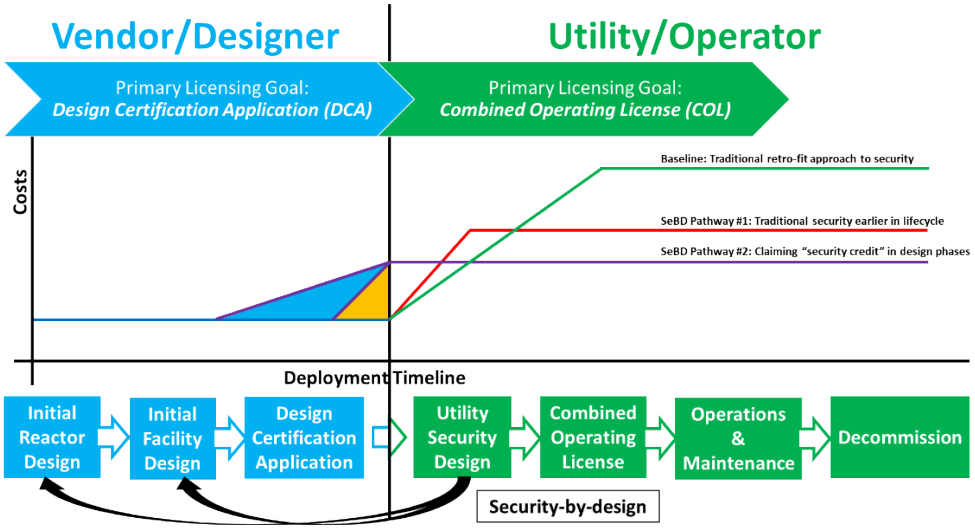

Figure 3. Comparing traditional security approaches to the proposed SeBD approach using a regulatory/engineering lifecycle model

In an attempt to clarify the arguments for this SeBD approach, consider the following notional example. A utility/operator anticipates spending $10 on retrofitting a DCA-licensed facility design to meet the security requirements of its COL—perhaps including an advanced detection capability. Now, assume there is part of the advanced detection capability that can be addressed by the designer during the DCA process that costs $2 (e.g., including additionally cabling trays or conduit around the facility's perimeter) that could reduce the anticipated retrofit by $5. If the designer chooses to make this pre-DCA design, they could increase the cost of the DCA-approved design to the operator—say by $3—to account for that extra $2 cost.

The result is a similarly effective security solution that potentially manifests:

- in a higher sale price for the designer—a $1 dollar increase in profit
- a reduced cost of meeting COL security requirements for the operator—$3 increase in DCA-licensed design + $5 in security retrofits for the COL = $8 total
- a reduced overall cost for security—$8 vs. $10 in pure retrofits

In addition to cost savings/sharing, seeking opportunities to claim "security benefits" from facility and safety design decisions made to support the DCA also presents opportunities for additional SeBD collaboration between designers and operators. Though still early in its development, this proposed regulatory and engineering lifecycle model approach provides increased clarity to support SeBD for A/SMRs, as demonstrated in current arguments being submitted to NRC in support of SMR licensing—including how:

> 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. [15, p. 13.6-1]

CONCLUSIONS & IMPLICATIONS

The driving factors behind developing this proposed regulatory and engineering lifecycle model approach stem from professional observations and experiences, as well as anticipated future needs for nuclear security. For example, SeBD approaches are well suited to mitigate the challenges facing protection of U.S. nuclear power plants after the 9/11 terrorist attacks [16]. Looking back, there are significant nuclear security system design, implementation and maintenance lessons that can be learned from operational experience. This proposed approach would allow such lessons to be incorporated earlier into development of a new nuclear facility, offering two pathways toward building SeBD based on past experience.

In addition, the two related pathways of SeBD offer several implications for domestic nuclear security requirements and international nuclear security best practices. Consider, for example, the opportunity to expand and refine international best practices across these two pathways of SeBD. While consistent with previous descriptions of SeBD, the first SeBD proposed pathway highlights the cost benefits of incorporating traditional security elements earlier in the lifecycle. Again, using the tradition of retrofitting security elements into nuclear facilities, addressing regulatory needs for security earlier in the lifecycle can reduce overall resources needed.

In terms of international best practices, this proposed pathway suggests an opportunity to map 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:

- Wall thickness and reinforced doors placed in credible adversary pathways
- Building designs capable of advanced technology deployment (i.e. hallway and ceiling dimensions that allow for remote operated weapon system deployments)
- Facility designs that force adversary paths to a choke point to increase response force effectiveness

In addition, the second proposed SeBD pathway—claiming security credit in the design phases of the lifecycle—offers additional cost reduction. Examples here include:

- Running extra conduit around facility and nuclear island perimeters to allow for easier deployment of future reactor modules and security technologies
- Security plan development for all planned reactor modules and key supporting systems
- Using modeling and simulation capabilities to inform plant design and configuration in each design stage of the facility to develop effective security systems that adapt with each facility design change

Where this proposed regulatory and engineering lifecycle model approach increases consensus and transparency for nuclear security decision-making, it directly supports calls for SeBD to helps incorporate security earlier, more frequently and continuously through domestic nuclear facility development. In response, this proposed regulatory and engineering lifecycle model approach offers a comprehensive framing of how to conceptually and practically achieve SeBD. By highlighting the trade-offs for addressing security requirements at different points in the lifecycle, this proposal approach helps identify—and hopefully optimize—SeBD decisions in a consensus and transparent manner across the vendor, utility, regulatory and nuclear security professional communities.

REFERENCES

[1] [1 Evans, A., et. al (2021). "U.S. Domestic Pebble Bed Reactor: Security-by-Design," SAND2021-13122R, Sandia National Laboratories, Albuquerque, NM.

[2] Liou, Joanne. (2021) "Safety by design: How the new generation of nuclear reactors addresses safety," *IAEA Bulletin* (Online), 62(1), pp. 18-19.

[3] Sevini, F., G. Renda, and V. Sidlova. (2011) "A safeguardability check-list for safeguards by design," *ESARDA Bulletin,* 46, pp. 79-84.

[4] International Atomic Energy Agency. (2011) "Technical Meeting on Safety, Security and Safeguards by Design for Small Modular Reactors," <https://www.iaea.org/events/evt2102735>.

[5] Snell, M.K. and C. D. Jaeger (2014) "Incorporating Security-by-Design in both Planned and Operational Nuclear Facilities" SAND2014-15268C, Sandia National Laboratories, Albuquerque, NM.

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

[7] International Atomic Energy Agency. (2011) "Nuclear Security Recommendations on Physical Protection of Nuclear Materials and Nuclear Facilities," *Nuclear Security Series No. 13 (INFCIRC/225/Rev5),* <https://www.iaea.org/publications/8629/nuclear-security-recommendations-on-physical-protection-of-nuclear-material-and-nuclear-facilities-infcirc/225/revision-5>.

[8] Garcia, M.L. (2008) Design and Evaluation of Physical Protection Systems, 2nd Edition, Boston: Butterworth-Heinemann.

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

[10] 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).

[11] 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.

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

[13] Nuclear Regulatory Commission (2020) "Stages of the Nuclear Fuel Cycle," <https://www.nrc. gov/materials/fuel-cycle-fac/stages-fuel-cycle.html> accessed on Mar. 28, 2022.

[14] Nuclear Regulatory Commission (2020) "New Reactor Licensing Process Graphic," <https://www.nrc. gov/images/reactors/new-reactor-licensing-process.gif> accessed on Mar. 28, 2022.

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

[16] Holt, M. and A. Andrews (2014) "Nuclear Power Plant Security and Vulnerabilities," Congressional Research Service Report for Congress RL34331.