INCORPORATING INTERNATIONAL CONSIDERATIONS INTO SYSTEMS ENGINEERING AND REGULATORY LIFECYCLE-BASED FRAMEWORK FOR SECURITY-BY-DESIGN

A.D. WILLIAMS, STEVEN HOROWITZ, ALAN EVANS
Sandia National Laboratories
Albuquerque, NM, USA
Email: adwilli@sandia.gov

K. HOLT
Office of International Nuclear Security, National Nuclear Security Administration
Washington, D.C., USA

Abstract

The popularity of advanced and small modular reactors (A/SMR) is driving "security-by-design" (SeBD) efforts. Current approaches range from applying traditional protection strategies "early in the design lifecycle," to seeking "intrinsic security … as an integral part of the organization," to making "security … [a] part of the facility lifestyle." Yet, international A/SMR considerations highlight an opportunity to recharacterize SeBD options. In response, the U.S. National Nuclear Security Administration's (NNSA) Office of International Nuclear Security (INS) and Sandia National Laboratories have developed an SeBD framework based on systems engineering and the regulatory lifecycle. This framework has two goals. First, it identifies opportunities that exist for achieving security goals at each A/SMR lifecycle stage. Second, it categorizes those SeBD options related to which stakeholder (including the designer or utility) might have primary responsibility. Consider, for example, the International Atomic Energy Agency's (IAEA) safety guide SSG-20. If SSG-20 is considered part of an engineering and lifecycle model of A/SMR development, then this SeBD approach should identify opportunities to claim credit for security performance that align with safety and operations-relevant A/SMR decisions described in SSG-20. The paper will use demonstration cases to describe this framework, as well as offer lessons insights for incorporating SeBD in—and improving security for—A/SMRs.

1. INTRODUCTION

The popularity of advanced and small modular reactors (A/SMR) is driving "security-by-design" (SeBD) efforts. For nuclear facilities, the State is responsible for ensuring a legal and regulatory framework against which security design and performance can be assessed to ensure protection from malicious attempts to leverage the harmful effects of radiation. In this regard, both safety and security play a vital role in regulatory decision-making toward licensing for certain activities, including siting, design, construction activities, commissioning, operation, and decommissioning. Increased interest in A/SMRs has driven an exploration into more efficient license decision-making. More specifically, there is a growing discussion around the hypothesized benefits of addressing security needs earlier in the A/SMR lifecycle. This so-called "security-by-design" initiative has several interpretations in the international discourse [1], including (but not limited to):

- "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"
- "intrinsic security … as an integral part of the organization … to provide a security margin proportionate to the risk without excessive disruption of business"
- "integration of security at the earliest stages to mitigate malicious acts, and [SeBD] should be part of the facility lifecycle."

These SeBD interpretations describe several potential advantages [1] to support the anticipated level of A/SMR deployment, including cost reduction (via the ability to demonstrate effective security performance before construction), inclusion of organizational and operational issues for commercial facilities (via the ability to better align security solutions with remote operation considerations), and, shifting from prescriptive to performance-

based for nuclear security evaluation (via the ability to reframe security requirements as operations requirements in design). Further, [1] identified an interesting common theme among these interpretations related to identifying and exploiting opportunities to address security needs early, frequently, and throughout an A/SMR's development lifecycle.

This concept is similar to ongoing discussions in the systems security engineering community looking to better incorporate security considerations into the foundational or core design requirements throughout a system's lifecycle. From this perspective, earlier lifecycle stages present greater opportunities to best address security needs without significant negative impacts to costs or operational efficiencies. Consider a recent example illustrating a systems security engineering approach to protecting space systems [2]. Efforts to identify opportunities to introduce security solutions earlier can emerge from evaluating a system's lifecycle (FIG. 1[A]). Similarly, this systems security engineering approach frames potential design solutions in terms of a trade space to aid decision-making (FIG. 1[B])—like that for A/SMR licensing.

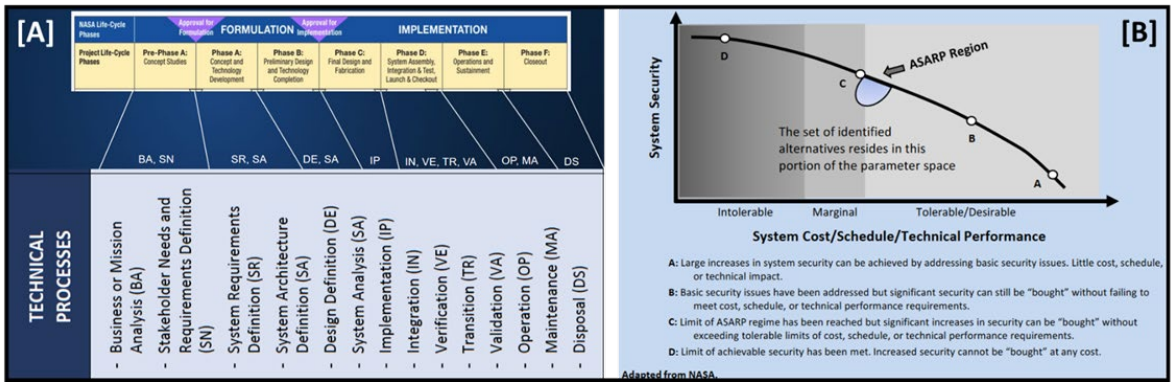

FIG. 1. A systems security engineering approach using a [A] lifecycle model to identify and include opportunities for addressing security needs and a [B] trade-space model to align decision-making, security solutions, and acceptable performance (from [2]).

Over the course of an engineering lifecycle, opportunities to efficiently address security needs are reduced (significantly) as operational characteristics and design decisions are finalized. From this perspective, the SeBD discussion can be reframed as shifting a focus to identifying—and leveraging—opportunities to claim security credit during traditional operation- and safety-related design decisions.

2. THE INS SECURITY-BY-DESIGN FRAMEWORK

In response, the NNSA's Office of International Nuclear Security (INS) has leveraged this lifecycle concept into a model for security-by-design (SeBD) [1]. Similar to the logic undergirding the systems security engineering perspective described in the previous section, the INS SeBD model focuses on identifying and exploiting opportunities to take security performance credit for operational decisions in the design lifecycle of commercial nuclear facilities. This INS SeBD model further builds on the lifecycle concept for developing both engineered systems and regulatory structures, as follows:

- *Engineered system lifecycle models* illustrate how decisions change in scale and scope as the design matures, map performance uncertainty versus evolving system maturity, and track cost-versus-performance tradeoffs from conception to deployment.
- *Regulatory structure lifecycle models* identify opportunities to standardize requirements (and highlight potential exceptions), illustrate impactful issues for regulatory development, and mitigate the potential for regulatory capture (a phenomenon occurring when independent regulatory bodies are (in)directly controlled by the industry they were created to oversee).

Taken together, these lifecycle models provide the structure to identify opportunities to incorporate desired security objectives early, frequently, and continuously.

The transparency offered by a lifecycle model-based approach to SeBD is particularly germane to A/SMR design and development. More specifically, earlier in a given lifecycle means the system is farther from being

fully realized, resulting in a higher degree of flexibility in updating requirements and design decisions—ideally to better match expected security performance for A/SMRs. For example, opportunities for SeBD will be larger in number and more diverse in options in the Pre-Phase A and Phase A portions of FIG. 1[A], where security credit can be explored in a stakeholder needs analysis or system architecture definition. Conversely, as the system becomes more fully realized (moving to the right in FIG. 1[A]), opportunities to change the requirements or designs to improve security are reduced (via validation in Phase D or Operation in Phase E, for example). In general, earlier in the lifecycle SeBD options emerge from modifying related requirements, but those options can quickly shift in focus to navigating within the requirements to meet desired security performance.

The common inclusion of feedback loops in lifecycle models reframes SeBD as a dynamic endeavor and enables continuing discussion on how to traverse the SeBD continuum from changing the design requirements (or constraints) to navigating within the design requirements (or constraints). More specifically, consider FIG. 2, which manifests this engineering and regulatory lifecycle model into an SeBD approach for A/SMRs. For simplicity and clarity, the lifecycle model offered in FIG. 1[A] is consolidated into the differing security-related responsibilities between A/SMR vendors (reactor designers and manufacturers) and potential A/SMR utilities (facility owners and operators). In general, A/SMR vendors are responsible for initial reactor and facility design, with the goal of receiving a certified design capable of being sold to utilities. Likewise, generic A/SMR utilities are responsible for translating a certified design into a deployed reactor and facility that is operated and maintained over its lifecycle (through decommissioning). (NOTE: Standards for each type of certification or licensing will be specifically defined by each country—though this generic model can be instructive and beneficial.)

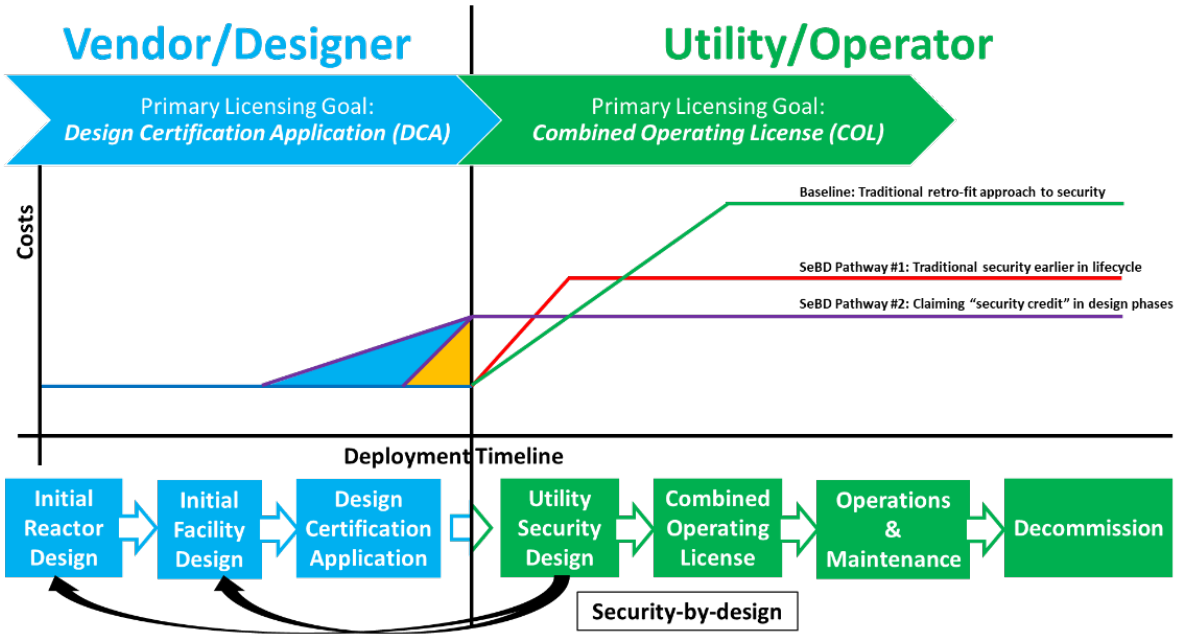

FIG. 2. Comparing traditional security approaches to the proposed SeBD approach using a regulatory/engineering lifecycle model, recreated from [1]

For additional explanation, consider a hypothetical A/SMR vendor and utility navigating the licensing requirements of the U.S. Nuclear Regulatory Commission (NRC). In this structure, the primary licensing goal of a generic A/SMR vendor is an approved design certification application (DCA), and the primary licensing goal of a generic utility is an approved combined operating license (COL). Tradition and observations indicate a strict separation of security-related responsibilities between vendor/designer and utility/operator (shown as a black vertical line between the "design certification application" and "utility security design" steps in FIG. 2). In many cases, this separation resulted in retro-fitted security solutions to the COL-approved facility design (the green lines labelled "Baseline: Traditional retrofit approach to security" on the right side of FIG. 2)—which also caused a majority of security costs to be assumed by the utility/operator

In contrast, the INS SeBD model (FIG. 2) illustrates two pathways for how security could be introduced earlier for this hypothetical A/SMR seeking NRC licensing—both before completing (the purple lines in FIG. 2) and soon after completion of the DCA (the red lines in FIG. 2). More precisely, these two pathways for taking security "credit" for safety and facility design decisions toward DCA or COL approval include the following:

— *SeBD Pathway 1:* The extent to which security regulations for the COL can be addressed during pre-deployment stages of the lifecycle
— *SeBD Pathway 2:* The extent to which COL security requirements can be addressed in the DCA by claiming "security credit" for safety and operations-related facility design decisions.

The two SeBD pathways in FIG. 2 illustrate how "security credit" can be successfully claimed closer to (or within) the DCA and offer several interesting outcomes. First, the INS SeBD model shows how costs for meeting desired security performance can be shared between vendors and utilities—reducing overall costs of a COL for the utility and (potentially) making a vendor's design more marketable. Second, there is significant opportunity for security credit to be claimed for pre-DCA safety and operations-related design decisions—similar to the concepts illustrated in FIG. 1[A]. For both of these benefits, the sizes of the teal and orange triangles on the left side of FIG. 2 represent the potential cost sharing or savings from each SeBD pathway. Lastly, the engineering and regulatory lifecycle ethos of the INS SeBD model provides a structured and iterative mechanism supportive of A/SMR stakeholder (including vendors, utilities, and regulators) coordination related to A/SMR technology, onsite nuclear material storage, site layout and plant operations.

3. INCORPORATING SEBD INTO INTERNATIONAL INSTRUMENTS

Currently, the International Atomic Energy Agency (IAEA) is developing its Nuclear Harmonization and Standardization Initiative to support potential A/SMR deployment. This initiative—and other IAEA documentation—will be helpful for identifying several potential opportunities for applying this INS SeBD model more broadly. In other words, applying the INS SeBD model within an international perspective emerges from focusing on understanding what elements of security performance can be identified and introduced in the current suite of IAEA documentation. For example, consider the IAEA Specific Safety Guide (SSG) "Safety Assessment for Research Reactors and Preparation of the Safety Analysis (SSG-20 Rev. 1)," which introduces, describes, and recommends content of the safety analysis report of research reactors [3]. (NOTE: Research reactors are used as a representative example for potential A/SMR facilities, given the similarities between fuel, size, and operational environment characteristics.) As such, this document provides a framework that aids identifying and inserting SeBD-based solutions, particularly through the 20 topical chapters suggested for the Safety Analysis Report (SAR) of a research reactor by the appendices of SSG-20 Rev. 1.

In terms of SeBD, SSG-20 Rev. 1 clearly states that the preparation of a safety analysis report should include "the understanding of the interface between safety and nuclear security [3, Pg. 20]" and "the design features of the nuclear security system (including physical protection and information security) that are important to safety [3, Pg. 35]." Additional, more detailed connections to SeBD in SSG-20 Rev. 1 include (but are not limited to) the following:

— *Chapter 2 (Safety Objectives and Engineering Design Requirements)* includes instructions to make "Provisions for interfaces between nuclear safety and nuclear security [3, Pg. 41]."
— *Chapter 13 (Conduct of Operations)* articulates a need to "describe the organizational structure and…conduct of operations for the research reactor…[to] include … interfaces with nuclear security [3, Pg. 81]."

Though representative, these more detailed examples indicate logical opportunities for the INS-supported SeBD model to be leveraged within an SSG-20 Rev. 1 process—working toward the inclusion of security solutions into design discussions of technological aspects of research reactors.

Further, INS SeBD model is one mechanism for how SSG-20 Rev. 1 calls for enhanced coordination between safety and security, namely the following:

> Safety measures and nuclear security measures are required to be designed and applied in an integrated manner, and as far as possible in a complementary manner, so that nuclear security measures do not compromise safety and safety measures do not compromise security [3, Pg. 84].

Additionally, consider Annex I of SSG-20 Rev. 1, which describes a range of suggested methods for safety analysis and includes identifying, selecting, and evaluating postulated initiating events and conducting event sequence analysis. As these different safety analysis techniques highlight potential misuse or undesired behaviors within the nuclear facility, they posit natural connection points to the INS SeBD model for exploring security-inspired requirements or solutions. Annex III's description of additional characterization of a research reactor facility—including (but not limited to) fuel parameters, shielding mechanisms, reactivity controls, and standard/off-normal/emergency operations—provide additional hooks into design decisions that can both inform (and be informed by) SeBD-identified security solutions.

Despite how SSG-20 Rev. 1 highlights the importance of security interfaces in research reactor design considerations, SeBD is not a requirement for IAEA or any international binding agreement. Yet, the underlying logic of SSG-20 Rev. 1 is conceptually and analytically consistent with the INS SeBD model. Consider, for example, the consistency between where SSG-20 Rev. 1 says that "safety analysis … should proceed in parallel with the design process, with iteration between the two activities … [and] should increase as the design process progresses [3, Pg. 23]" and the description of the INS SeBD model as "a rigorous, structured, and iterative mechanism for exploring various security solutions [1, Pg. 9]." Please see Table 1. as a representative sample of results from applying this INS-supported SeBD model to SSG-20 Rev. 1.

TABLE 1. Summary of applying INS SeBD model to SSG-20 Rev. 1 recommendations for a research reactor safety analysis report (where recommended chapter descriptions are offered in the Appendix)

Safety Design Recommendations [SSG-20 Rev. 1, Chapter # provided in the Appendix]	Related SeBD Consideration(s)
Research Reactor Cooling Systems & Connected Systems [Ch. 6] *Engineered Safety Systems* [Ch. 7]	Redesigning systems, structure and components to incorporate security performance
Instrumentation and Control Systems [Ch. 8]	Reanalyzing diverse, reliable, and redundant pressure valves to address potential manipulation
Operational Radiation Safety [Ch. 12]	Investigating nuclear material accounting and control solutions to be aligned with the frequency and assaying procedures of research reactor waste streams
Conduct of Operations [Ch. 13]	Incorporating security considerations into crystallizing regular research reactor facility operations

Ultimately, increased coordination of the INS SeBD model and IAEA safety documentation (like SSG-20 Rev. 1) can paradigmatically shift the focus toward accomplishing desired performance via a structured and iterative mechanism to claim security credit for each operational (and safety) decision made to ensure a design meets acceptance criteria.

4. CONCLUSIONS & INSIGHTS

Even though demonstrated on notional research reactor design considerations, this lifecycle concept-based SeBD model shows promise—and feasibility—for investigating, identifying, and characterizing how security credit can be leveraged in facility operational (and safety) design decisions. The INS SeBD model also helps focus on evaluations to claim security credit along a potential system lifecycle of an A/SMR—particularly in terms of

the range of technical parameters, initial conditions, and safety analysis methods suggested in the SSG-20 Rev. 1. For example, the SeBD suggestion to re-analyze diverse, reliable, and redundant pressure valves to address potential manipulation both aligns with the call to ensure the "adequacy of the protection system to shut down the reactor in a safe manner (e.g., by providing redundancy and diversity)" outlined in SSG-20 Rev 1.'s proposed SAR Chapter 8 (provided in the Appendix) *and* could be modified and applied to other A/SMR designs. In this manner, the INS SeBD model will likely be similarly applicable to future IAEA safety guidance for A/SMRs—even if based on *different* safety analysis report structures.

More specifically, the extent to which the SSG-20 Rev. 1 report structure is aligned with a generic system lifecycle model for an A/SMR indicated the utility of numerous opportunities for addressing security needs through technical, functional or procedural solutions. According to SeBD pathway 1, for example, traditional nuclear security solutions can be applied earlier in the developmental stages, after a design-based certification is offered. Likewise, SeBD pathway 2 helps showcase how nuclear security solutions can emerge in design phase and take advantage of both operational requirements and safety mitigations. This INS SeBD model is also suited for iterative applications and can support more detailed safety analyses that may be required in a regulatory process. Ultimately, the INS SeBD model seeks to provide a balanced solution to optimize security needs and navigate away from the tradition of expensive, operationally-intensive, and retroactive security solutions.

Though representative in nature, the efficacy of this INS SeBD model indicates the basis of a structured and iterative process for improving security performance for future nuclear facilities (see [4], for example). Extrapolating from the categorical similarities between research reactors and A/SMRs (e.g., disparate types of operational environments, range of anticipated thermal outputs and radiological inventories), indicates that the benefits of the INS SeBD model could be experienced more broadly. Even the preliminary comparison of the INS SeBD approach to IAEA's SSG-20 Rev. 1 demonstrate a strong start for building a more robust and practical methodology for SeBD. Next steps potentially include:

- Continuing the R&D collaboration with interested A/SMR partners to refine the SeBD model
- Expanding the comparative analysis with additional safety and operational reporting best practices (including from the IAEA, World Association for Nuclear Operators, Institute of Nuclear Power Operators, etc)
- Collaborating with international partners to enhance the feasibility and utility of the SeBD model

To support the current interest in—and anticipated deployment levels of—A/SMRs, the INS SeBD approach offers three benefits. First, it seeks to rigorously, justifiably, and systematically identify—and even optimize—security solutions for A/SMRs. Second, the INS SeBD model can help designers and vendors incorporate security needs earlier, more frequently, and continuously in A/SMR development. Lastly, the INS model encourages SeBD consensus, transparency, and (possible) cost-sharing across the vendor, utility, regulatory, and nuclear security stakeholders. Taken together, the advantages of the INS SeBD model can support widespread deployment of A/SMRs in a responsible, safe, and secure manner.

ACKNOWLEDGEMENTS

The authors would like to thank various experts from across NNSA's Office of International Nuclear Security program for contributing to the evolution of the SeBD framework. Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC (NTESS), a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration (DOE/NNSA) under contract DE-NA0003525. This written work is authored by an employee of NTESS. The employee, not NTESS, owns the right, title and interest in and to the written work and is responsible for its contents. Any subjective views or opinions that might be expressed in the written work do not necessarily represent the views of the U.S. Government. The publisher acknowledges that the U.S. Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this written work or allow others to do so, for U.S. Government purposes. The DOE will provide public access to results of federally sponsored research in accordance with the DOE Public Access Plan. SAND2024-07759C.

REFERENCES

[1] WILLIAMS, A.D. and A.S. Evans (2023) “Enhancing a Systems Engineering and Regulatory Lifecycle-Based Framework for Security-by-Design,” Proc. of the Joint INMM & ESARDA Annual Meeting, Vienna, Austria.

[2] ROSS, R. (2023) “Next Generation Mission-Based Security for Systems Engineers,” Comp. Sec. Resource Center, Nat. Inst. Stand. & Tech., <https://csrc.nist.gov/Presentations/2023/next-generation-mission-based-security-for-systems>.

[3] INTERNATIONAL ATOMIC ENERGY AGENCY (2022) “Safety Assessment for Research Reactors and Preparation of the Safety Analysis Report: Specific Safety Guide,” IAEA Safety Stand. Series No. SSG-20 (Rev. 1).

[4] WILLIAMS, A.D., et. al (2024) “Incorporating International Security-by-Design (SeBD) Approach for Molten Salt Research Reactors,” Proc. 65th INMM Ann. Mtg, Portland, OR.