# Recommendations for Design-STAGE Safety and Security Probabilistic Risk Assessment Co-Development

Alexander J. Huning

Oak Ridge National Laboratory

Oak Ridge, USA

Email: huninghj@ornl.gov

Steve J. Reed

Oak Ridge National Laboratory

Oak Ridge, USA

**Abstract**

As many advanced and small modular reactor developers are entering the licensing process and seeking to expand their commercial offerings internationally, nuclear security is a critical but often overlooked element in the design process. Probabilistic risk assessments (PRAs) are being used to support risk-informed safety assessments but have not gained significant awareness as highly effective multi-purpose tools for a broad range of nuclear security applications. Designing a plant protection system and other barriers that might serve a security function after a conceptual or basic design phase may lead to higher total security costs and/or redesign of other buildings, structures, and system placements or components. This motivates a “security-by-design” approach. PRAs can supplement this approach by aiding in identifying and quantifying the risk importance of various target sets and assessing the impact or consequences of security scenarios, thereby improving the protection strategy to adequately address the risks due to all design basis threats. However, there are many fundamental differences between a PRA used for safety and one used for security events (i.e., sabotage events). When these differences are identified and included in the development processes, a coupled safety and security PRA can be effectively constructed without placing significantly more burden on the design and analysis teams.

Using traditional PRA elements as a guide, this paper provides technical recommendations for the integration of security and plant protection features into a safety PRA, which can easily be turned on or off depending on the application. The goal is to create an effective and integrated safety and security PRA model without having separate models, thereby eliminating version control and consistency problems to which design phase risk assessments are vulnerable.

## INTRODUCTION

Recently, the Nuclear Energy Institute (NEI) conducted a survey [1] and found that operating costs for existing US reactors represent a significant fraction (62% in 2021) of the total cost for nuclear electricity generation ($29.13/MWh in 2021). Although operating costs have indeed declined since peaking in 2012, both fuel and capital costs have declined by greater margins. Security costs have increased since 2008, which can be attributed to the shift in physical security postures toward a more labor-intensive approach [2]. This is an unsustainable approach for most advanced and small modular reactors (A/SMRs); these reactors are challenged by reduced power levels, requiring a reduced security staff level to simply maintain existing cost fractions. This has motivated a security-by-design (SeBD) approach to reduce the reliance on labor-intensive approaches; incorporate more passive security features; appropriately credit passive safety features, including a reduced radionuclide inventory (hazard) associated with both A/SMR and microreactor systems; and leverage the recent advancements in intrusion monitoring and detection systems.

Any successful SeBD approach will integrate with the safety design strategy; this is colloquially referred to as a *2S approach*. Additionally, many designs being considered for international deployment are also developing flexible design features for the incorporation of safeguards for an integrated “3S” approach. Methods for the incorporation of international safeguards are beyond the scope for this discussion; however, safeguards should not be overlooked, as the placement of instrumentation and inspection capabilities may impact both physical security and safety system layout and design.

In the United States, probabilistic risk assessments (PRAs)—or probabilistic safety assessments (PSAs) internationally—have been used successfully across the operating fleet to demonstrate levels of adequate protection for a host of different applications, including but not limited to reduced maintenance costs and scheduling, risk-informed tech specs, reduced operator staffing, reduced site and emergency planning boundaries, appropriate safety classification of systems, structures, and components (SSCs), and defense-in-depth (DID) adequacy evaluations. For nuclear security, PRAs have been used successfully to inform the target set selection and consequence evaluations for security scenarios. SeBD approaches leveraging PRA will be able to identify target sets more appropriately at an earlier stage, leading to more optimized and efficient physical protection system (PPS) designs that do not rely on labor-intensive approaches.

Many A/SMR concepts are employing a design stage PRA to meet their licensing and regulatory goals or for seeking risk-informed benefits from those applications listed above. However, emphasis should be placed on including some PPS and other features that may not normally be included in a safety-only PRA so as to effectively use the PRA for SeBD approaches. For regulatory acceptance, PRAs generally need to meet standard requirements that are judged through peer-review and other assessment processes. For non–light-water reactor (LWR) PRAs, the ASME/ANS RA-S-1.4-2021 [3] standard is generally followed. A range of PRA applications are considered for this standard. However, nuclear security threats and features for nuclear security are excluded from consideration by the standard and its working group. This decision was primarily derived from the host of LWR PRA standards by which the non-LWR standard was heavily influenced. In those LWR PRA standards, security threats are also excluded. It should be noted, however, that this exclusion does not represent an inherent technical obstacle or fundamental deficiency in the PRA development process. It is unclear whether a full standard is necessary for nuclear security PRA development. However, at the very least, additional guidance is needed to appropriately consider security threats in the development of a non-LWR PRA. This will allow for some consistency across non-PRAs for security applications and to assist peer reviewers and regulators in their assessment of the PRA and its applications. This paper explores some observations and provides recommendations for the integration of security considerations during PRA development.

### Target Set Identification

Target sets are the foundation of a reactor site’s security strategy. Traditionally, safety-related equipment along with logic models developed from support system failure analysis, cable routing, and flooding information are used to identify the set of potential targets that require protection. From this potential list, security and consequence domain expertise is employed to screen and finalize the target sets. This methodology is explained in greater detail in regulatory guide (RG) 5.81 revision 0 [4]. However, this approach has many drawbacks that are referenced and rectified by employing a PRA as outlined in RG 5.81 revision 1 [5]. This new revision is not perfect either and has some drawbacks itself, specifically for design stage reactors and A/SMR concepts under development. Some considerations of using the PRA-based approach include:

* Risk ranking and prioritizing based on how achievable or desirable each target set is remains subjective and largely requires expert knowledge of specific scenarios and the techniques adversaries would employ.
* Consequences associated with the destruction, or functional failure, of each potential target set could be different due to the highly dynamic nature of an attack from a standard safety scenario. These attack scenarios may impose boundary conditions and assumptions not originally considered in the deterministic safety calculations. This may lead to some non-conservative exclusion of target sets.
* No inclusion of safety and security by design in the quantification and formulation of potential target sets.

### SeBD

SeBD is broadly defined as follows:

 “…*the system-level incorporation of the PPS into a new nuclear power plant or nuclear facility resulting in a PPS design that minimizes the risk of malicious acts leading to nuclear material theft; nuclear material sabotage; and facility sabotage as much as possible through features inhere in (or intrinsic to) the design of the facility”* [6].

For advanced reactors, SeBD is expected by advanced reactor developers and is documented in the Commission Policy Statement:

“*The goal of the policy statement update is to encourage advanced reactor designers to consider safety and security in the early stages of design in order to identify potential design features and/or mitigative measures that provide a more robust and effective security posture with less reliance on operational programs”* [7].

Additionally, the NRC-proposed rule for 10 CFR Part 53 includes a requirement for safety and security in the design process:

*“Safety and security must be considered together in the design process such that, where possible, security issues are effectively resolved through design and engineered security features”* [8].

How SeBD is implemented will depend on the reactor technology and organization or vendor performing the design efforts. Design and evaluation processes for achieving SeBD have been developed [6]. However, questions remain about the development costs, benefits, and articulating the need for a SeBD business case, which may include the requirement for constructing a PRA depending on the method selected for identifying target sets and other security analyses. Like the target set methodology question, the INSTAR program is investigating the SeBD business case and is promoting the need for 2S and 3S within the developer community. To achieve SeBD, additional guidance is needed for integrating security considerations to the PRA during the development and evaluation processes. The next section highlights some elements where integration is necessary.

## 2S PRA CO-DEVELOPMENT CONSIDERATIONS

This section describes some practical considerations for PRA development in terms of standard PRA elements both safety and security applications. The presented recommendations may not be applicable depending on the specific reactor technology or design, or the level of design information available. The general approach to 2S PRA co-development is presented in Fig. 1.



*FIG. 1. 2S PRA Development Methodology*

### Considerations Following PRA Technical Elements Approach

A full listing of each high level and supporting level requirement from the non-LWR PRA standard and their assessment for nuclear security applications is beyond the scope of this paper. It is recommended that vendors committing to PRA development and SeBD during a conceptual design phase be cognizant of standard requirements and perform their own assessment of applicable requirements as they relate to PPS risk-informed design applicability and other security applications, such as target set identification. This section is intended to represent a starting point for future evaluation.

The most significant modification, which has been heavily documented [9,10], is the modification of the risk equation associated with an event or event sequence “i”, R(i), from Eq. 1a to Eq. 1b. This substitution of event sequence frequency information, f(i), with a desirability or attractiveness concept, d(i), is necessary for several reasons. Firstly, it is performed to eliminate any attempt at quantifying a likelihood of attack that requires time-dependent law enforcement information and/or state intelligence. Secondly, the switch to a desirability or attractiveness allows for more generic, time-independent feedback and decision-making capability for the designers.

|  |  |
| --- | --- |
| $$R\left(i\right)=f\left(i\right)∙c\left(i\right)$$ | (1a) |
| $$R\left(i\right)=d\left(i\right)∙c\left(i\right)$$ | (1b) |

In Eq. 1a and 1.b, the consequence, c(i), of some scenario “i” primarily includes the radioactivity release and offsite dose potential associated with the reactor core. However, A/SMRs may also include risk and security evaluations for non-reactor core sources and other hazards. These consequence evaluations are not likely to significantly change in their approach when considering security scenarios. However, the desirability value is open to debate and subject to re-evaluation when new information about evolving threats is obtained.

To implement this modification and other aspects of the PPS design, some standard PRA element modifications are recommended and are listed below.

### Plant Operating State Analyses

For A/SMRs, plant operating states (POSs) may be more complex than traditional LWR operating states due to a variety of factors, including load following at reduced power levels as a consistent or normal operation state, on-line refueling, component modularity or replacement during normal operation, combined process heat and electricity production modes, black start operation, remote vs. on-site operations, and other novel reactor features. To facilitate the integration of PPS design and security features, additional plant operating states due to security events should be investigated if security measures involve shutting down equipment or altering component states that are not already modeled under an existing plant state. If security procedures prescribe plant state changes, then this new plant state may be more resistant to acts of sabotage, but it could also expose vulnerabilities associated with standard reliability failures or pre-existing conditions that could increase accidental risk. If security measures involve transitioning into an existing plant operating state (e.g., hot standby) with no additional SSC state modifications, then no further assessment is likely necessary.

### Initiating Event Analysis

The objective of initiating event analysis is to identify a reasonably complete list of initiating events, to group events into manageable sets with similar mitigation requirements, and to attached frequencies to those groups. For nuclear security applications, an analysis of initiating events of malicious origin (IEMO) is typically performed. Broadly, IEMOs include two categories not typically included in LWR safety PRAs: (1) events with exceedingly low frequencies that are screened out but could be induced via some malicious action, and (2) sabotage of non-core sources of radioactivity [11]. For item (2), this consideration is now included across many different supporting requirements in the non-LWR PRA standard (e.g., IE-D1). For item (1), PRA developers should ensure that passive system failure initiating events that may have been justifiably screened from a random failure perspective are considered as potential failures in a sabotage event.

### Event Sequence Analysis

As alluded to earlier, it is critical that event sequence analysis consider or not inherently screen out or dismiss exceedingly low probability events that may be achievable absent successful mitigation or interdiction. One recommendation would be to include a pre-event tree or similar logic model that captures critical aspects of the various security scenarios of interest (i.e., design basis threat scenarios) and address how those aspects translate to or impact the set of safety event sequences. For example, is off-site power assumed to fail in every event?

Special consideration should also be applied to places in the event sequences where (a) human operator actions play a significant role, (b) timing and phenomenological thresholds are built-in to the event sequence modeling, (c) a combined internal fire and flood scenario arises, and (d) repair or recovery paths are modeled. Items (a) and (d) are relatively easy to include for security scenarios and build in an option or flag for quantification of these events. Items (b) and (c) may require structural changes to the event sequence models. For example, are branches used for different component or system operability (e.g., splits in the fault tree or event trees for different system or component performance values)? Are these branches sufficient, or could security scenarios introduce or emphasize branches that have not been considered?

### Success Criteria

Success criteria are, naturally, difficult to define adequately for security scenarios given the broad spectrum of potential events and available strategies to mitigate such events. Generally, for any design basis threat, the plant protection systems are required to be “effective” for a certain time to allow for state or other law enforcement support. Due to threat-specific (e.g., site- and country-specific features) and radiological consequence factors, no further elaboration or generic recommendations can be provided. However, it is reemphasized that no event sequence in the PRA inherently eliminates events that could be influenced by malicious actions. Modeling and simulation and other engineering basis calculations for these types of events are beyond the scope this paper but may be necessary to develop adequate protection strategies.

### Desirability Modifications (Systems, Data, and Quantification Elements)

For these elements, several modifications are needed to incorporate security along with reliability and safety events. These modifications are primarily located in the system fault trees where a sabotage, cyber, or other insider attack could threaten a system or component, as shown in Fig. 2. Quantification would be performed either on only the security events or on the safety events, but not both.



*FIG. 2. Example system fault tree modifications for security assessments*

Quantifying system fault trees and, ultimately, the event sequences for security risk applications will require modifications to the basic event data typically used for safety assessments. Principally, this includes assigning a desirability factor for each added security basic event. This factor is then relative to other plant components, and it enables the ranking of “higher risk” scenarios or cut-sets without ranking specially on probability or frequency, which is informally verboten. If a fire or flood event can be initiated in an area, then depending on the threat (i.e., adversary capabilities), some distinction would need to be made between disabling an area as compared to disabling an individual component within that area.

Finally, cut-sets could be screened for modeling or estimating risk posed by specific threats (e.g., drone attack). Screening would be performed if too many adversarial tasks or individual components fail, which would be estimated as beyond the assumed adversary capability.

When assessing quantification, one challenge is then assigning truncation limits that are too high. Some legitimately high-risk scenarios could be well under what is typically quantifiable for safety scenarios. One example is that where several components have individually low desirability factors but, because of their proximity or other common cause attribute, may as a group form a high desirability factor. Because desirability may be calculated or assumed using a variety of different and mostly subjective methods, modeling and simulation, as well as domain knowledge, will play a significant role in risk integration and assessment of these scenarios or cut-sets. However, to investigate their potential as a case for PPS design, target set identification, or other security application, they must be first quantified and then identified from the PRA results.

### Source Term and Consequence Analyses

With respect to radiological health consequences, security scenarios present unique challenges that typical safety analyses do not consider. For example, any explosive or other accelerant not normally present in the plant that is introduced will have the potential to cause additional dispersal of radiological materials beyond what is normally physically possible. However, a systematic process can be established for A/SMRs that do not use core damage type metrics. Two principal options are identified and are illustrated in Fig. 3.



*FIG. 3. Example options for source term and security consequence analysis*

The first option is to expand each end state from the safety PRA considering an adversary’s capabilities (i.e., design basis threat or DBT) and each variation that could either mitigate or increase the radionuclide release. Then, disposition of each new end state is performed to eliminate repetitive or end states with similar expected consequences. The second option is to inject additional DBT and adversary actions at the applicable event level in the event tree. These would not add top events but rather add options or multiple branches to those existing events by informing how those events fail depending on the adversary actions. Disposition is then automatically performed during event construction. For either option, knowledge of potential adversary actions capabilities is necessary for accurate consequence assessment. Although not directly illustrated in Fig. 3, the “OK” or “SAFE” end states should also be re-evaluated as well.

Finally, the tools used for estimating the release magnitudes and composition should account for the additional explosive, accelerant, or other chemical or physical process introduced by the adversary corresponding to the end states identified through a process like that shown in Fig. 3.

### Other Elements

In addition to those elements discussed, internal fire and flood models may require significant modifications for sabotage-related events. Like the example shown in Fig. 2, similar modifications could be made in those fault trees for area fires and floods. If there is a deviation in expected consequences from the safety PRA, then those consequences could be modeled in the event tree using either option described earlier.

Uncertainty analysis for security risk assessment may also be more challenging because desirability and consequence values rely heavily on expert judgement. Therefore, sensitivity studies may be more important here than they are for traditional safety risk assessments, to assess where data and knowledge are needed to ensure that the selection of target sets is correct and to ensure that protection strategies are effective at preventing any high or unacceptable radiological consequence.

Risk integration is potentially more challenging for security events as importance measures are more subjective and typically do not include any measure of the effectiveness of the designed security strategy. Any PRA result can then be used to help define the security strategy, but that effectiveness measure is not typically reintegrated into or considered in the PRA. Even if this were performed, new scenarios would become important, but it would have no impact on the expected effectiveness until those exercises (simulation or tabletop-based exercises for design stage A/SMRs) could be performed. No standard or industry-accepted “desirability-consequence” or other risk metric target exists for security events. Even if security risk metrics were standardized, it is unclear how they could be appropriately weighted against frequency-oriented safety risk metrics.

## CONCLUSIONS

This paper presents some initial considerations for integrating security elements into the construction of a safety PRA to improve PPS design and to develop efficient protection strategies at an earlier stage as well as for any other risk-informed A/SMR security application. The goal of a PRA is to answer questions related to the risk triplet: “what can go wrong,” “how likely is it,” and “what are the consequences?” Identifying “what can go wrong” is expected to be more efficient when security and safety PRAs are developed in unison. Expert resources may only need to be tasked once, with minimal associated overhead, with relearning model decisions and assumptions. This is especially apparent for system fault tree model development. If a component may fail due to some malicious action, then it can then be investigated simultaneously for a natural equivalent failure mode or effect.

For security assessments, all likelihood and probabilities related to the threats are replaced with a desirability value. This desirability value is heavily subjective, and various approaches can be used to weight or rank equipment for security evaluations. Several options are presented herein for integration of security scenarios into consequence assessment and binning. Other elements for risk integration and uncertainty analysis are identified as potential gaps and require additional work for developing new methods or guidance.

**ACKNOWLEDGMENTS**

The authors would like to thank the sponsor, DOE NNSA office of nuclear non-proliferation, International Nuclear Security for support and attendance at the IAEA’s 2024 International Conference on Small Modular Reactors.

**REFERENCES**

1. Nuclear Energy Institute, Nuclear Costs in Context, (October 2022).

<https://nei.org/CorporateSite/media/filefolder/resources/reports-and-briefs/2022-Nuclear-Costs-in-Context.pdf>

1. Burli, P. H. and Yadav, V., Economic Analysis of Physical Security at Nuclear Power Plants, Idaho National Laboratory, INL/EXT-20-59737, Revision 0, (September 2020).
2. The American Society of Mechanical Engineers and The American Nuclear Society, Probabilistic Risk Assessment Standard for Advanced Non-Light Water Reactor Nuclear Power Plants, ASME/ANS RA-S-1.4-2021, (February 2021).
3. U.S. Nuclear Regulatory Commission, Target Set Identification and Development for Nuclear Power Reactors, Regulatory Guide 5.81, Revision 0, (November 2010).
4. U.S. Nuclear Regulatory Commission, Target Set Identification and Development for Nuclear Power Reactors, Regulatory Guide 5.81, Revision 1, (December 2019).
5. SNELL M. K. et al., Security-by-Design Handbook, Sandia National Laboratories, SAND2013-0038, (January 2013).
6. U.S. Nuclear Regulatory Commission, Policy Statement on the Regulation of Advanced Reactors, NRC-2008-0237, 73 FR 26349, (May 2008).
7. U.S. Nuclear Regulatory Commission, PART 53 – Risk-Informed, Technology-Inclusive Regulatory Framework for Commercial Nuclear Power Plants, Subpart C – Design and Analysis Requirements, Sec. §53.440, Design Requirements, SECY-023-0021: Enclosure 1 – Proposed Rule Federal Register Notice, ADAMS Accession No. ML21162A102, (March 2023).
8. HUNING, A. J. and HARRISON, T. J, Methods for the Enhancement of Security Probabilistic Risk Assessments, Oak Ridge National Laboratory, ORNL/TM-2021/2023, (March 2021).
9. NELSON, S., JAIN, P., and HUNING, A. J., Security by Design: A Plant Design and Component-Based Approach to Technical Solutions to Insider and Outside Threat, Oak Ridge National Laboratory, ORNL/TM-2023/2850, (May 2023).
10. VARNADO, G. V., and WHITEHEAD D. W., Vital Area Identification for U.S. Nuclear Regulatory Commission Nuclear Power Reactor Licensees and New Reactor Applications, Sandia National Laboratories, SAND2008-5644, (September 2008).