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

TOWARD A NEW APPROACH FOR VITAL AREA IDENTIFICATION FOR CUTTING-EDGE NUCLEAR FACILITIES

Adam D. Williams, Andrew J. Clark, Alan Evans and Jesse J. Bland
Sandia National Laboratories*
Albuquerque, NM, USA, adwilli@sandia.gov

ABSTRACT

Current best practices in vital area identification (VAI) focus on preventing radiological sabotage in terms of damage to reactor cores and spent fuel during a range of distinct operational states. Given that radiological sabotage results in the same types of undesirable radiological releases as a nuclear accident, there is a significant amount of hazard and risk analysis that these VAI approaches leverage from regularly completed safety assessments. More specifically, these approaches translate event-tree and fault-tree models into potential sabotage logic models that identify various areas within a facility that those potential sabotage actions might occur. Yet, several trends in commercial nuclear facilities—such as increased digitization; non-traditional fuel cycles. including novel chemical and physical fuel forms; passive or inherent safety elements, and novel in-plant activities—are challenging the efficacy of such approaches.

Particularly when considering new issues faced in achieving design certification for "advanced" or "modular" types of reactor designs, new approaches to VAI should be explored. In response, Sandia National Laboratories is investigating the efficacy of new analytical approaches to better meet today's VAI needs. One new approach seeks to leverage "Master Logic Diagram (MLD)" models—a top-down logical structure designed to determine required facility functions—to help coordinate security-related insights from across data sources to support VAI. Similarly, systems theoretic process analysis (STPA)—a hazards analysis technique based on systems and control-theory—has attractive analytic characteristics to enhance VAI. Building on the structure of traditional VAI, the new approach captures more comprehensive (and non-linear) relationships between structures, systems. and components—supporting more efficient and effective VAI-related design decisions.

After briefly summarizing the traditional approach to VAI and highlighting areas of improvement, this paper will introduce several new analytic concepts poised to address this improvement area. Next, this paper will describe how these concepts can form a new VAI approach and will demonstrate its effectiveness with several anecdotes. Lastly, this paper will discuss conclusions, insights, and implications of the proposed VAI approach to support design and deployment decisions for nuclear facility security solutions.

* **SAND2023-02880 C**, 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

Current best practices in vital area identification (VAI) focus on characterizing the radiological assets or material and their protection/control systems that could be used to create a radiological sabotage event in terms of reactor-core and spent=fuel damage during a range of distinct operational states. Given that radiological sabotage results in the same types of undesirable radiological releases as a nuclear accident, there is a significant amount of hazard and risk analysis that these VAI approaches leverage from regularly completed safety assessments. In other words, VAI plays an integral role in adequately and accurately characterizing security risk related to nuclear facility operations. Rather than evaluate the systems, structures, and components (SSC) related to nuclear accidents, vital areas refer to locations within a nuclear facility that house critical operational elements that must be protected to prevent radiological sabotage.[1]

A widely cited reference [2] serves as the *de facto* state-of-the-art for conducting VAI for nuclear facilities. This VAI approach effectively translates event-tree and fault-tree models into potential sabotage logic models that identify various areas within a facility where those potential sabotage actions might occur. Such models are reviewed to identify the combination of areas—called target sets—that adversaries must logically visit to produce radiological releases of concern. These results are also evaluated to organize and prioritize the combinations of areas that *must* be protected to *prevent* radiological sabotage—the so-called "vital areas." Identifying vital areas can help streamline the design and deployment of security systems and solutions for nuclear facilities.

This traditional VAI approach is graphically summarized in Figure 1. Per [2], VAI consists of the following high-level steps (restated for brevity):

1. Identity all inventories of radioactive materials and include each in the sabotage logic model
2. Determine if direct dispersal is possible (if so, include each as an event in the logic model)
3. Identify all initiating events (IE) that could result in radiological sabotage
4. Identify all systems (and success criteria) required to mitigate the IEs above
5. Develop the sabotage logic model to capture indirect avenues to radiological sabotage
6. Eliminate any event from the sabotage logic model not included in the design basis threat (DBT)
7. Identify and replace the events in the sabotage logic model with the corresponding areas
8. Solve the sabotage "area" logic model to identify target sets for radiological sabotage
9. Determine the corresponding prevention sets for the sabotage "area" logic model
10. Select the vital areas that will be protected to prevent radiological sabotage

The popularity of this VAI approach has been crystallized in its incorporation into the IAEA Nuclear Security Series [3], which provides additional context for completing each step.

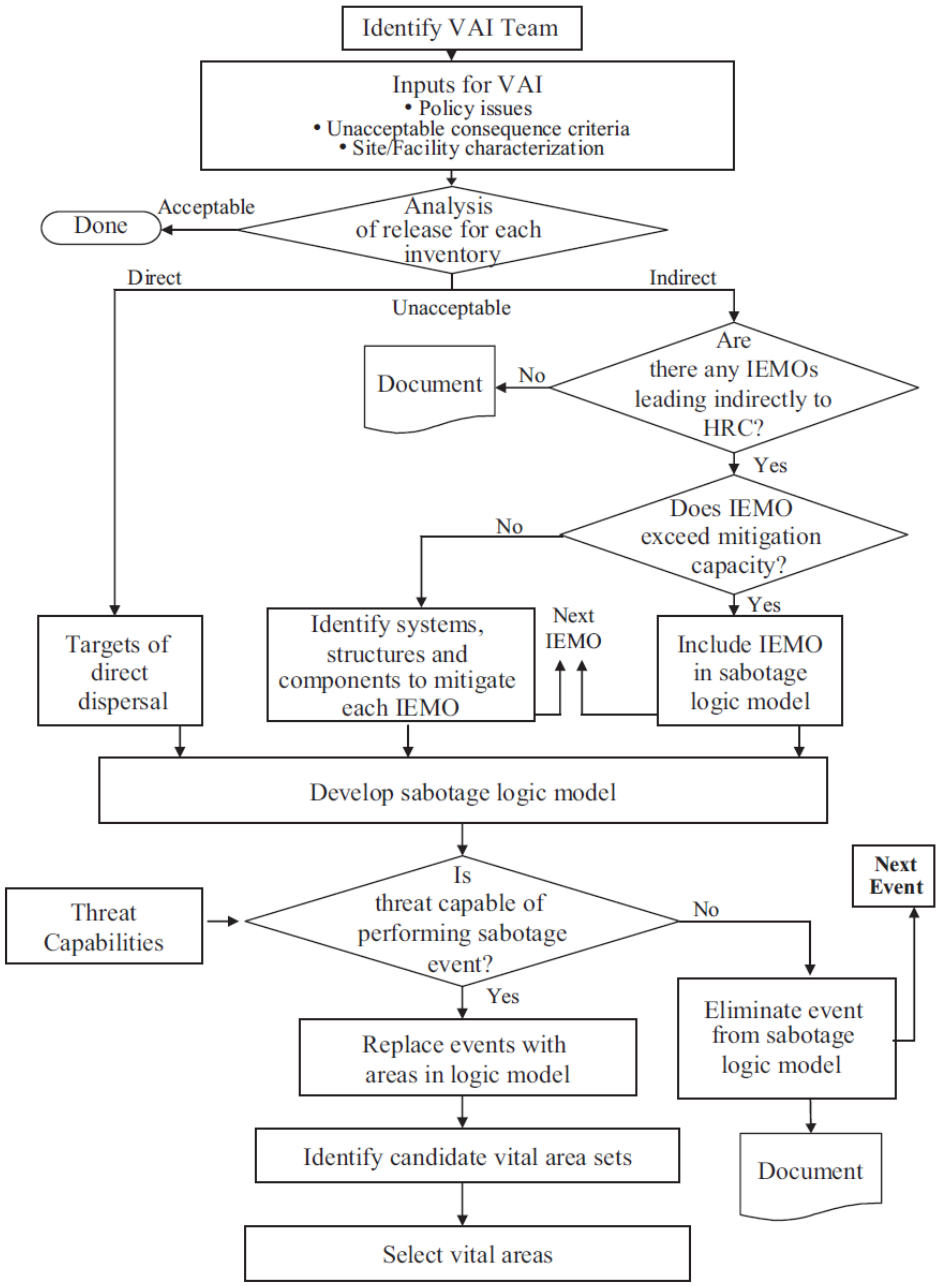

Figure 1. Graphical description of the *de facto* state-of-the-art for VAI, from [3].

While Figure 1 visualizes the VAI process as a decision tree, there are a few key *analytical* considerations to highlight. First, steps 3 and 4 from the preceding list inherently assume analytical completeness—namely that "all" relevant initiating events (IE), including a comprehensive set of initiating events *of malicious origin* (IEMO), are identified. For clarity, if a relevant IE or IEMO is *not identified* and thus *not included*, then the corresponding SSCs will not be named, nor will the associated list of related areas that must be protected to prevent radiological sabotage.

Second, if probability-based fault-tree models for safety analysis are used as the basis for steps 3 and 4, then it is important to note some crucial differences in sabotage logic models that use fault trees. As the focus shifts from failure modes and mechanisms to the location of an SSC corresponding to the failure event, typical interpretations of "failure mechanisms" will also change. Particularly in the context of IEMOs, detailing specific potential adversary actions (the security equivalent of "failure mechanisms") is less important than identifying that an IEMO or disabled SSC is *possible*. Consider, for example, needing to identify the existence of remote operation of a pump from the control room versus more precisely how an adversary might manipulate control of that pump. Further, the challenge of comprehensively describing possible adversary actions with the same degree of confidence as "failure mechanisms" in nuclear safety suggests a potential need to revisit SSC behaviors screened out of PRA-based analysis because they were deemed "too unlikely" to occur.

Lastly, this VAI approach was originally developed for traditional large-scale nuclear power plants based on light water reactors. Over the years of its implementation, this VAI approach has been optimized to meet the needs of the current fleet of nuclear power facilities based on light water reactors. Analytically, this approach has resulted in a long-standing assumption that "all core damages are created equal"—a statement that helps clarify and simplify initial steps in building the sabotage logic model. Yet, in practice this assumption removes some SSCs from the VAI that may be crucial for limiting intentional radioactive release in a risk-informed manner. By implication, advanced reactors[1]—including but not limited to pebble-bed reactors and molten salt reactors—may not use such a blanket "core damage" end state for VAI. Rather, advanced reactors might seek to define their consequences in a more nuanced and refined manner, particularly given new opportunities for risk-informed, performance-based, technology-inclusive methodologies for non-light water reactors (see [4] for more details on risk-informed, performance-based, technology-inclusive guidance).

Security cost reduction may be achieved by improving the resolution of the location and characterization of the site's vital areas. Advanced reactor sites will have fundamentally different systems that protect against—and control for—the release of radionuclides to the environment. By leveraging these differences through new approaches to VAI, advanced reactor facilities may be able to reduce the size of some vital areas, thus improving the efficiency of associated security systems. Examples of novel approaches to VAI will be discussed in the remainder of this paper.

VAI CONSIDERATIONS FOR CUTTING-EDGE NUCLEAR FACILITIES

Several trends anticipated in advanced nuclear facilities—such as increased digitization, non-traditional fuel cycles, passive/inherent safety elements, and novel in-plant activities—may challenge the efficacy of traditional VAI approaches. As introduced in the preceding section,

[1] Here, the authors are referring to reactor facilities that look starkly different from the current large-scale, light water reactor-based facilities—whether in terms of size, mobility, or primary reactor technology. In some dialogues, these assumptions are lumped into such phrases as "small modular reactors," "advanced/small modular reactors," or "novel and advanced reactors." The International Atomic Energy Agency's *Advanced Reactor Information Systems* service (https://aris.iaea.org) provides a useful summary of these technologies.

these unique challenges to the traditional VAI approach also serve as opportunities to develop an enhanced VAI approach more aligned to advanced reactors.

Where the manner for identifying IEMOs employed by traditional VAI approaches is vague, ambiguous, and incomplete, inputs for identifying IEMOs can come from a range of potential sources. This ambiguity provides an opportunity to help correct tendencies within current VAI approaches that erroneously center on and conflate IEMOs with *only* safety-analysis derived "postulated initiating events." Moreover, insight from additional data sources—such as VAI reports for similar facilities (if available), engineering evaluation reports, and deductive analysis—can augment such common tendencies and improve on describing IEMOs for advanced reactors.

To further visualize the analytic difference in completeness between IEs and IEMOs described above, consider the range of design interfaces and dependencies anticipated in advanced reactor facilities. In one example, the steam turbine system—including the notional cooling tower—would be susceptible to loss of steam generator feedwater, an IE likely identified in safety analysis (and germane as a top event for several other event sequences [ESQ[2]]). If the steam turbine system was located within the turbine building, then the turbine building itself might be labeled a vital area. Yet, the cooling tower itself may *not* be identified as being related to this IE in the safety analysis and thus be excluded. However, an adversary action against the cooling tower could lead to the same IE—suggesting a potential vital area that is left out of the analysis. In another example, the electrical system architecture for advanced reactors is important based on the expectation that there will be cross-ties and switches outside of safety analysis-identified areas of concern (e.g., "control" or "electrical" buildings). Here, potential IEMOs against switchyard- and transformer-related equipment at the advanced reactor facility outside of these previously identified might also be vital areas in need to protection to mitigate the IE "loss of offsite power."

According to international best practices [3], the potential sabotage areas identified should be evaluated against the DBT. One goal of this step is to justify removing any IEMOs (or ESQs) beyond the expected capability of the regulatorily defined adversary—which, in turn, may result in a smaller number of vital areas to protect. Yet, the ability to complete this step is challenged, given that many advanced reactors are in varying stages of design and thus details on related regulatorily defined adversary capabilities may not be accessible in the near term. In response, there seems a need for a different approach to down-select IEMOs based not on the potential success of adversary action but on potential consequences to the facility.

One conceptually similar mechanism for eliminating IEMOs or ESQs relates to taking credit for security benefits offered by other facility design decisions. Consider, for example, if an advanced reactor facility offers more ballistically resistant building materials as an additional layer of security around the entire reactor building. In this manner, understanding how facility design

[2] For clarity, "event sequences" (ESQ) consist of two parts. One is the "accident sequence" (AQ) that describes how the plant responds to an undesired action that matriculates through the nuclear facility. Second is the "initiating event" (IE) that describes the first undesired event that the plant needs to respond to in order to prevent a consequence. Since "initiating events of malicious origin" (IEMOs) are derived from IEs, ESQs are used to describe outcomes from fault-tree based sabotage (area) logic models.

strategies—like enhanced building materials—mitigates or deters *any* adversary capability to execute IEMOs or ESQs can help identify and categorize vital areas. If all areas of concern (and their associated SSCs) within this hypothetical reactor building have such an extra layer of security, then the related priority as vital areas decreases.

Conceptualizing VAI for advanced reactor facilities also challenges how traditional VAI approaches focus on ESQs that result in core damage. Given the anticipated operations of many advanced reactor designs—those that are "passively" or "inherently" safe—connecting VAI to core damage represents a misplaced focus for undesired consequences. Enhancements in VAI, should then emphasize modern risk-informed and performance-based analytical techniques that are better capable of assessing a spectrum of undesired consequences. For example, a qualitative scale that ranks consequences for license basis events from intact (e.g., no expected offsite dose from a related radiological release) to high (e.g., the highest expected offsite does from a related radiological release) could be used to both identify and categorize vital areas. In this regard, advances in VAI are well positioned to shift toward a graded consequence approach to help down-select event sequences and systems to produce more detailed sabotage logic models.

A NEW APPROACH FOR ENHANCED VAI

Given the challenge of incorporating all the passive SSCs and phenomenon anticipated in advanced reactor facility operations, the popular tactic of reviewing and leveraging already existing risk assessment documentation may be incomplete. In response, a refined Master Logic Diagram (MLD) approach is offered as an alternative approach to identifying IEMOs. MLDs have a long history of use in nuclear safety, feature top-down/deductive processes (which are often visualized as fault trees), and can help coordinate IEMO-related insights from across data sources. This top-down logical structure for determining required facility safety functions necessary to prevent radiological release helps categorize a wide variety of potential IEMOs without having to arbitrarily screen out "highly unlikely" events. This observation suggests that MLDs could create new and more efficient process flows for the iterative (and complicated) process for determining if an IEMO exceeds capacity—as well as more insights into what mitigating SSC exists to counter a given IEMO.

These same logic structure capabilities of MLDs also serve a mechanism for capturing nuanced safety features (and therefore the related IEMOs) of advanced reactors that are not commonly included in traditional PRA assessments (or if they are included, are often a source of model uncertainty that is difficult to characterize). For clarity, consider separating nuclear facility safety features into three categories:

- Active SSCs
- Passive SSCs
- Inherent SSCs

Where traditional PRA assessments have been historically optimized to help identify *active* SSCs, there is not currently a consensus approach for adequately incorporating *passive* or *inherent* SSCs. An early version of implementing MLDs to better incorporate passive and inherent safety features for VAI is illustrated in Figure 2.

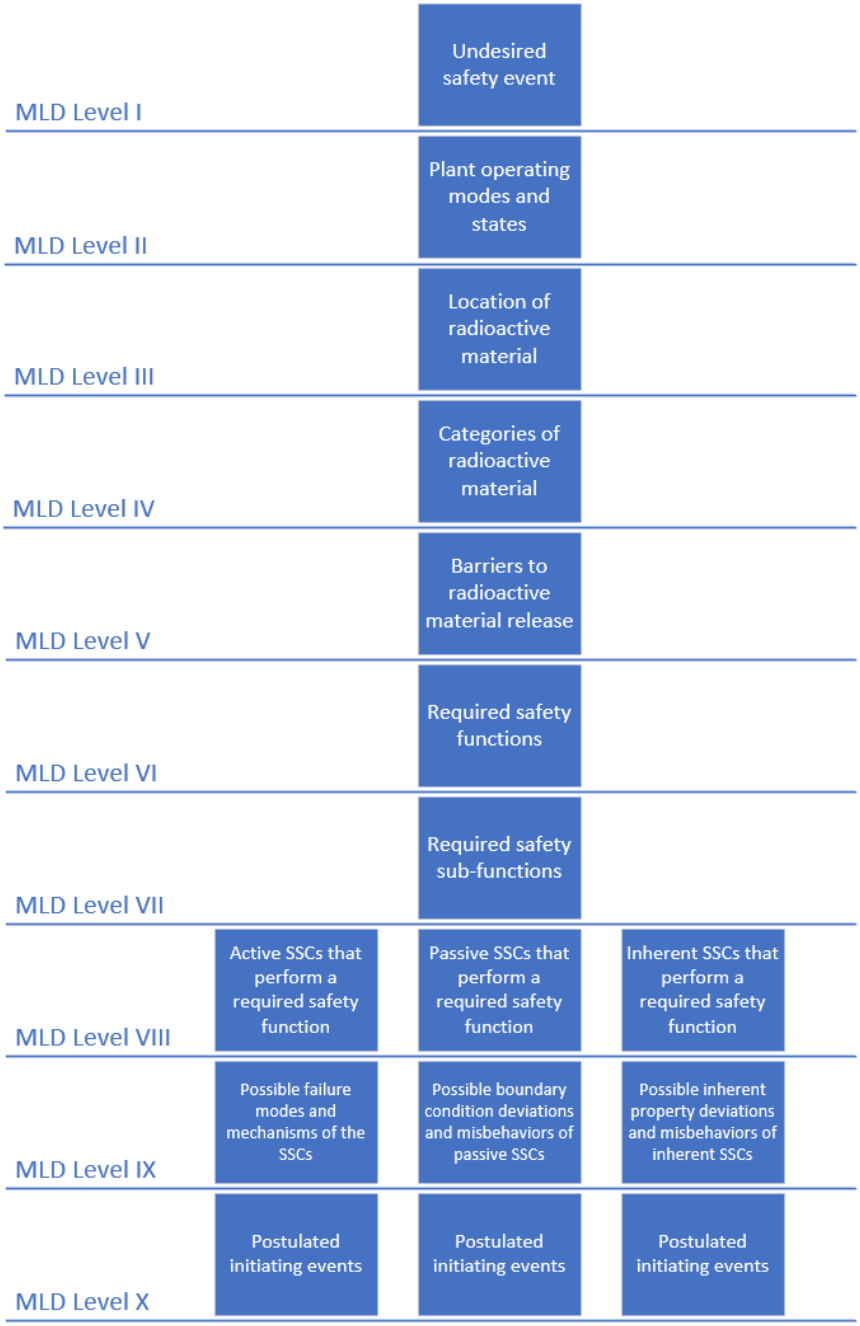

Figure 2. Graphical representation of an MLD-augments VAI approach. (Note that direct sabotage IEMOs are addressed in Level V while indirect sabotage IEMOs are addressed in Level VIII-X)

The ability to explicitly incorporate both passive and inherent SSCs into the VAI process will yield more complete and comprehensive sets of both IEMOs and vital areas. Preliminary exploration of this approach resulted in a more structured process flow for navigating assumptions of "completeness" for safety analysis-based results and the assumption that all IEMOs are created equal. Figure 3 below visualizes the categorical descriptions of radiological

materials within an advanced reactor facility as they are aligned with MLD levels I–IV. This traceability in analysis helps mitigate several of the challenges of advanced reactors to traditional VAI approaches and offers enhanced evaluative clarity. In addition, MLDs are a form of structured inquiry that offers two distinct advantages. First, MLDs can both help streamline (and enhance) technical and design decisions for advanced reactors facilities. Second, MLDs can better position safety and risk analyses to address the challenges of passive, inherent, and digital SSCs anticipated in advanced reactor facilities.

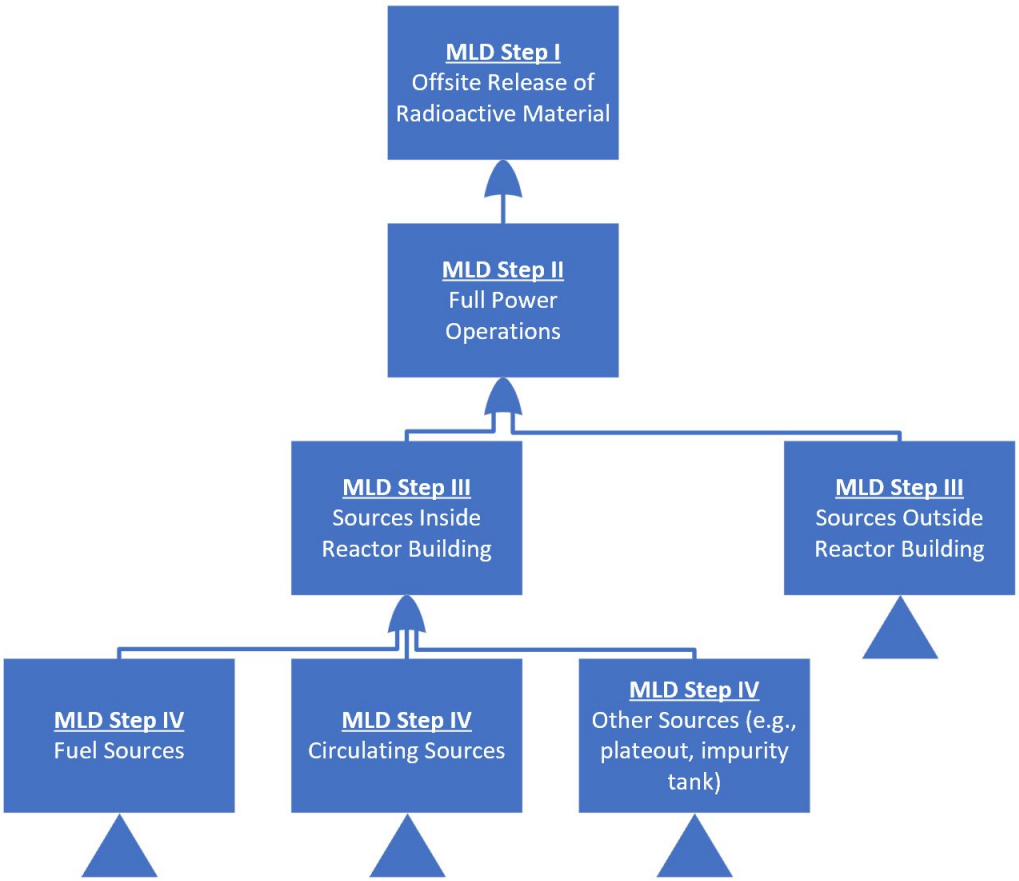

Figure 3. Graphical summary of the MLD steps I through IV for radiological sources within the reactor building of a notional advanced reactor facility.

CONCLUSIONS, INSIGHTS & IMPLICATIONS

The ultimate use of VAI results is to support design and deployment decisions for advanced reactor facility security solutions. Incorporating MLDs into VAI approaches can help provide equivalent "risk" analysis for *indirect* ESQs impacting radiological sources outside of the safety analysis-identified areas of concern. Similarly, shifting the focus from DBT-based decisions to a consequence-based down-selection process provides an iterative process for modifying traditional VAI approaches to non-traditional and early-state advanced reactor design that is commensurate with modern PRA approaches (e.g., NEI 18-04 [4]). Similarly, these new elements can help identify (and guide) areas of increased security credit for early facility design

decisions—like potentially repositioning passive or inherent SSCs to leverage their protective capacity to reduce the number of vital areas. By invoking MLDs and a consequence-based paradigm, VAI can be augmented to systematically identify and categorize IEMOs with higher efficacy and enhanced completeness realtive to traditional approaches. Additionally, this systematic approach will enable an agile and efficient assessment technique as DBTs are identified and change with time.

These postulated benefits of introducing more "top-down" elements also introduce the ability to leverage insights from analysis techniques with similar logical structures. For example, systems-theoretic process analysis (STPA) is an increasingly popular approach for evaluating safety and hazards (e.g., "risk of undesired behaviors") in complex systems.[5] From its philosophical basis in systems theory, STPA combines concepts from systems and control theory—hierarchy, emergence, constraints, and feedback—to shift the conversation from "preventing an accident" to "enforcing system control." STPA analysis yields undesired variations of control actions necessary to maintain expected system operations and behaviors. Given that STPA is not restricted to quantitative thresholds, this list of undesired control actions provides two unique opportunities. First, they are a mechanism for efficiently evaluating sabotage concerns *beyond* those associated with core damage (which is the focal point in the traditional VAI approach). Second, the broad range of STPA-derived undesired control actions is a more comprehensive ability to explore potential adversary actions in a manner *not* restricted by considering regulatorily-defined adversary capabilities.

Building on these conceptual similarities with MLD—and prior success in aligning STPA results with fault-tree analysis [6]—STPA may be able to further enhance VAI approaches for advanced reactor facilities. More specifically, consider how traditional VAI "converts" basic events to target areas in a systematic manner. If adequately identifying adversary-initiated basic events is currently limited (as described above), then there is a need to address the restrictions on this process. The ability of STPA to identify areas and items of concern (often missed by traditional approaches) could be invoked as a mitigation. Early work in a similar exploration of STPA added undesired control actions as new top-events in fault trees and prioritized the associated basic areas (as converted basic events) on their frequency of appearance.[7] The associated results suggest that including STPA in VAI provides several key insights. First, this logic helps overcome previous challenges of missing potential vital areas related to adversary actions not included in DBT-focused evaluations. Second, the logic can identify candidate vital areas concurrent with the safety analysis development (rather than post-hoc as is traditionally done). Third, doing so can organize and prioritize an increased number of candidate vital areas in a quantitative manner *without* defaulting to probabilities. Lastly, these insights taken together suggest that augmenting VAI with MLD *and* STPA can help advanced reactor designers (and potential vendors) evaluate and mitigate vital areas earlier in their developmental process and across various stages of the design, construction, and operation of advanced reactors.

The conclusions and insights from exploring how MLDs and STPA can address challenges that advanced reactor facilities present to traditional approaches to VAI imply a need for further investigation. While early results are positive, incorporating these new adaptations into traditional VAI processes should be exercised on increasingly sophisticated use cases—ideally ending with adoptions by an advanced reactor vendor and national regulatory bodies. Building

on the structure of traditional approaches to incorporate these new analytical elements can enhance VAI by capturing more comprehensive (and non-linear) relationships between SSCs and more comprehensively identify IEMOs—which ultimately enable more efficient and effective VAI decisions in support of successful advanced reactor facility deployment.

REFERENCES

[1] U.S. NUCLEAR REGULATORY COMMISSION (1988). "Vital Equipment/Area Guidelines: Vital Area Committee Report (NUREG-1178)," Washington, D.C.

[2] VARNADO, G. AND D. WHITEHEAD (2008) "SANDIA REPORT: Vital Area Identification for U.S. Nuclear Regulatory Commission Nuclear Power Reactor Licensees and New Reactor Applicants (SAND 2008-5644)," Sandia National Laboratories, Albuquerque, NM.

[3] INTERNATIONAL ATOMIC ENERGY AGENCY (2012) "Technical Guidance: Identification of Vital Areas at Nuclear Facilities (NSS-16)," Vienna, Austria, <https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1505_web.pdf>.

[4] NUCLEAR ENERGY INSTITUTE (2019) "Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development (NEI 18-04, Rev 1),"Washington, D.C.

[5] LEVESON, N. (2012) Engineering a Safer World: Systems Thinking Applied to Safety, MIT Press, Cambridge, MA.

[6] CLARK, A.J. and A.D. Williams (2019) "Addressing Cyber Hazards in Nuclear Power Plants with Systems Theoretic-Informed Fault Trees" Proceedings of the 60th Annual Meeting of the Institute of Nuclear Materials Management, Indian Wells, CA.

[7] SANDT, E. (2022) "Exploring Vital Area Identification Methods Using an Adversary-Inclusive Version of Systems Theoretic Process Analysis," PhD Dissertation, Ohio State University.