ORNL/LTR-2024/7

ORNL Peer Review Summary and Recommendations for *Advanced Reactor Designs Security Analysis, Risk, and Recommendations:*

Risks, Consequences, and Possible Design Mitigation Approaches Associated with Select Advanced Reactors Study

Adam Smith
Scott Nelson
Alex Huning
Steve Reed
Mohamad Zineddin
Samantha Sabatino

February 2024

OAK RIDGE National Laboratory

ORNL IS MANAGED BY UT-BATTELLE LLC FOR THE US DEPARTMENT OF ENERGY

ORNL/LTR-2024/7

Nuclear Energy and Fuel Cycle Division

ORNL PEER REVIEW SUMMARY AND RECOMMENDATIONS FOR

ADVANCED REACTOR DESIGNS SECURITY ANALYSIS, RISK, AND RECOMMENDATIONS: RISKS, CONSEQUENCES, AND POSSIBLE DESIGN MITIGATION APPROACHES ASSOCIATED WITH SELECT ADVANCED REACTORS STUDY

Adam Smith
Scott Nelson
Alex Huning
Steve Reed
Mohamad Zineddin
Samantha Sabatino

February 2024

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, TN 37831
managed by
UT-BATTELLE LLC
for the
US DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

ORNL Peer Review Summary and Recommendations

The purpose of this document is to provide a summary of the peer review conducted for the *Advanced Reactor Designs Security Analysis, Risk, and Recommendations: Risks, Consequences, and Possible Design Mitigation Approaches Associated with Select Advanced Reactors* study prepared by researchers at Idaho National Laboratory (INL), Argonne National Laboratory (ANL), and Oak Ridge National Laboratory (ORNL). The National Nuclear Security Administration (NNSA) International Nuclear Security (INS) program team requested that ORNL perform a peer review of the study report prior to publication as a final peer check before distributing the report to a broader audience.

A team of independent subject matter experts (SMEs) was identified to support the review with their various backgrounds in advanced reactor technologies, risk methods, safeguards, and security. Each review team member brings a unique perspective to the team, drawing from experience working for utilities, vendors, private industry, academia, and other research institutions. To ensure that the end user / stakeholder has a clear understanding of the report contents and its potential applications, the objectives for the review team were defined as follows:

(1) Confirming that the purpose and intended use of the document is clear
(2) Identifying when and how to use the report
(3) Ensuring that the methodologies presented are well defined and flexible enough to be adapted to the breadth and depth of advanced reactor (AR) technologies currently under development
(4) Identifying potential gaps or information within the study that could benefit from additional clarification, documentation, or references
(5) Providing constructive feedback to the authors in the spirit of continuous improvement
(6) Supporting the development of tools and resources for the broader INS community and its partners to support the safe and secure deployment of advanced nuclear technologies

Deliberately, the review team was not provided with any background information regarding the purpose or reasoning behind this work other than the fact that it was planned for use within the INS community. General themes and recommendations identified during the review are summarized in Table 1 for the authors' consideration. Other specific, detailed comments from the review team were recorded using track changes within the Microsoft Word document.

Overall, the ORNL Review Team is of the impression that the authors have made significant contributions toward what is recognizably a monumental task. The number of different reactor types, physical sizes, fuel forms, fuel cycles, user applications, and design maturity all contribute to the complexity of characterizing the safety and security of these technologies. It is impractical for any single document to include all the necessary details of every advanced reactor design technology being developed and then to identify all specific associated security risks. However, investors, government policy makers, and nuclear newcomers unfamiliar with these technologies could benefit from selected information presented in this study.

Conversely, it is the review team's opinion that SMEs, vendors/designers, regulators, and other experienced nuclear agency representatives may only glean a limited value from the methods and results because of the largely qualitative, highly subjective rankings presented in the subject document. Although a one-size-fits-all approach for the methodology has merit, it also comes with limitations that must be clearly defined for the target audience. This document will benefit from a more clearly defined purpose and better definition of the target audience, along with more information detailing the appropriate use for the results being developed.

Furthermore, it is unlikely that a fair and equitable selection of either a reactor technology or a specific vendor can be made using the presented high-level ratings. It is also unlikely that significant security conclusions can be drawn about a specific reactor design or vendor because implementation details and design information can drastically alter the outcome of the generic assessments made throughout the document. Recognizing that this may not be the document's purpose, the intended application of these methods must be clarified further, and direction should also be provided to avoid potential pitfalls.

It is recommended that the document be revised to address the feedback provided herein prior to formal release. Additionally, because of the combination of security information generated, the review team also advocates for withholding this report from public release, recommending that it must remain sponsor controlled. Considering the industry perspective, release of a document highlighting security risks by reactor type—even generically—could prove problematic for vendors and designers alike and may also imply that one technology is superior to another. Although the information used has been compiled from public sources, the document combines and screens the information into vulnerabilities. Additionally, information contained within this resource could be used to exploit advanced reactor technology risks. Additional derivative classification review and discussion with the INS sponsor is recommended.

A follow-on review of the updated document will be supported if the schedule for this deliverable permits. The ORNL Review Team appreciates the opportunity to support this review and looks forward to collaborating more on future work.

Table 1 – General Recommendations

#	Category	Observation	Notes	Suggested resolution
1	General	Information sensitivity	The report includes potentially sensitive security information regarding target sets, target vectors, and so on, which may necessitate withholding the report from public release. Although the authors have acknowledged that the information was collected from publicly available sources, the compilation makes it a single resource for security-related information for several advanced reactor technologies.	This is a gray area, so it is recommended that the authors work with the local derivative classifier (DC) review team and INS sponsor before public release.
2	General	Mission/problem statement	The intended audience, purpose, and "big picture" are all missing from the report. It is not clear what the reader should do with the methodology being presented, what the next step is, or how this all fits together with security by design (SeBD). What is the mission statement or problem being solved here? How should the reader use this report in the context of SeBD?	The report could benefit from a short, single-page introduction to set the stage for all the information being presented and how it should be used. First, discuss the intended audience (assumed to be INS partners/nuclear newcomers), and then talk through the big picture and overall plan. Specifically state the purpose of the report, how it fits into the plan, and how it is intended to be used, or how it fits into the next steps.
3	General	SeBD definition	SeBD, as it is intended to apply here, should be fully defined early in the document. Then, an explanation is needed to detail how this report is intended to be used in the context of SeBD. Examples in the text include addition of another safety system train for redundancy, for example. This is not so much SeBD as it is adding defense-in-depth.	It is recommended that the authors define SeBD and then how the tables/results can be used to accomplish it. It all ties back to audience and purpose. Who is the intended audience, and what is the problem that is being solved with this methodology?
4	General	SeBD vs. SSeBD	SeBD is already an abbreviation that is not well understood or defined within the industry. Do the authors really want to muddy the waters more by adding another new term and abbreviation, "safety and security by design (SSeBD)," within INS? In general, this document refers to these two abbreviations together at each instance as "SeBD and SSeBD." Purposely separating them as two unique approaches that should be integrated under the true intent of SeBD seems problematic and unnecessarily complex.	It is recommended that the authors stick with SeBD only—a single abbreviation—and acknowledge that safety is an integral part of a comprehensive SeBD methodology.

#	Category	Observation	Notes	Suggested resolution
5	General	SeBD and SSeBD	Page 1 of the Introduction immediately separates the Physical Protection System (PPS) from SeBD and SSeBD. Line 108 reads, "This study focuses on the inherent technology design aspects of SeBD and SSeBD and not the plant physical protection system (PPS)." If designers plan to implement technology design aspects of SeBD and SSeBD, then they must fundamentally integrate this with PPS technology throughout the design lifecycle (planning, design, construction, and operation). To instead add or fit the PPS technology in at a later stage would cause bigger problems and additional cost.	Clarification should be added to note that the approach to PPS is an integral part of SeBD and SSeBD.
6	General	Objective and goal	In general, the report states that AR developers, end users, and regulators apply the knowledge and methodology gained from this report to identify SeBD and SSeBD. However, developers, end users, and regulators already have more in-depth knowledge than presented in this report. Also, it is not clear when, how, or why the reader would use these methods for SeBD and SSeBD.	Clearly define the target audience and the purpose of the report from the outset. How is the information derived from these methods intended to be used, and how is it used in the context of SeBD?
7	General	Construction and operational stages	A stated goal is to increase facility resistance to attack during construction and operation. How? As stated in the report, the SeBD and SSeBD concepts during construction and operation are different than they appear during the facility design stage.	The authors should define what is meant by SeBD and SSeBD, or eliminate the second abbreviation, as previously suggested, and then articulate how these methods can be applied throughout the stages of the design lifecycle: planning, design, construction, and operation.
8	General	Security risks	How does one protect the security vulnerabilities of the systems, structures, and components (SSCs) identified through these methods?	It is recommended that further clarification explaining how to accomplish SeBD for identified security vulnerabilities be added. How is the information derived from these methods intended to be used, and how is it used in the context of SeBD?
9	General	Security risk reduction	In the report, recommendations to increase facility robustness include limiting access to reactor containment and spent fuel areas through SeBD changes. What does the report recommend to limit access by SeBD? What is meant by this statement?	Define what this looks like in practice. What changes can be incorporated to meet the intent of SeBD?
10	General	Cyber security and SeBD	The report mentions cyber security concerns but fails to recommend how to integrate cyber security with SeBD. Cyber security must be addressed during SeBD and SSeBD design stages.	It is recommended that the authors add additional information/clarification on how cyber security aspects can be integrated with SeBD and SSeBD.

#	Category	Observation	Notes	Suggested resolution
11	General	Methodology concerns	Are these release events occurring during a security event or during a typical safety perturbation? The design basis threat (DBT) is not actually defined in the report; instead, the DBT is defined as being consistent with 10 CFR 73.1.	It is recommended that the authors define the DBT early in Section 4.0, and then identify when the radiological releases are expected to occur in Section 4.3.
12	General	Methodology concerns	There is no discussion on the combination of failures that lead to core damage or dispersal. One of the major concerns in SeBD is equipment location.	The authors should address and discussed what leads to core damage or dispersal further in the report or acknowledge this as a limitation.
13	General	Methodology concerns	Intended use: It is important to note that this study does not account for vendor-specific design features that will help mitigate some of the highlighted risks. There is potential that INS partners and newcomers will use these findings to make technology decisions, so the authors must be careful about someone using this material as a basis for defining one technology as safer and more secure than another without the full picture. This is also related identifying the intended audience and ensuring that the intended use of these methods is clear from the outset. Risks are highlighted (1) to ensure that vendor-specific design features mitigate those risks, and (2) to identify areas that would benefit from application of SeBD features.	More clear and concise statements should be included in this document, especially considering the potential language barriers throughout the INS community. Suggestion: “The risks that result from the methodologies presented in this document are intended to be used to...[insert benefits/reasons here]. This document is not intended to be used to rank AR designs or to endorse any specific technology as being more safe or secure than others.’
14	Technical	SeBD is a complex process of embedding security into the full lifecycle of the selection, planning, design, construction, commissioning, operation, and decommissioning phases of a nuclear facility.	SeBD requires proper analysis, physical security infrastructure design and construction, technology selection, design, validation, installation, maintenance, policies and procedures, and manpower.	At a high level and at the outset of the report, the authors must clearly identify where, what, how, and at what level SeBD will be implemented into programs, processes, people, procedures, and plant equipment.
15	Technical	AR categories/ buckets: HTGR vs. GFR category and alignment with international community	In Section 3 and again in Section 5, high-temperature gas-cooled reactor (HTGR) is defined as a standalone category of advanced reactor types. The Generation IV International Forum (GIF) defines this category as gas-cooled fast reactors (GFRs) and includes HTGRs as a subset of GFRs.	For consistency with the international community, it might be worth aligning with the GIF categories and terminology, or at least noting that HTGRs are part of the broader GFR category used in other forums.

#	Category	Observation	Notes	Suggested resolution
16	Technical	US-Centric/NRC Focus	The document is US-centric and focuses primarily on US Nuclear Regulatory Commission (NRC), US Department of Energy (DOE), and US Environmental Protection Agency (EPA) regulations. If this document is intended to apply to the international community and INS partners, then it should at least acknowledge that different regulations exist and address why US regulations were considered in developing the methods. Where equivalency can be drawn, incorporating references to international regulations may help INS partners better relate to the US regulations being presented.	It would be worth adding a paragraph or two to acknowledge the differences between US regulations being cited and different regulations around the world. The document could also be updated to include references to the International Atomic Energy Agency (IAEA) survey of different international regulations to provide additional context. The key is to associate the US-based methods driven by US regulation and US requirements to foreign partners and foreign regulations. It should be clear how our INS partners can adapt these tools for their own use and/or their country-specific regulations.
17	Technical	Clear methodology identity	The methodology being presented throughout the document is referenced in many ways. It is referred to as a "security analysis methodology," an "adversary sabotage methodology," a "security risk qualification methodology," a "security risk analysis," and as a "risk assessment methodology." Although it may be all those things, determining and defining one term or phrase for this early on, and sticking with it throughout the report, would greatly improve readability.	Although it is often beneficial to vary vocabulary throughout a document to keep the reader engaged and avoid repetition, it has the potential to be confusing, especially when considering language barriers with an international audience and some of our INS partners. It is recommended that the authors standardize key terminology and apply it throughout the document in text and tables.
18	Technical	Next steps not clear – how to compile and use the information being generated	Once the methodology is established and explained, the color-coded tables are developed and presented, and high, medium, and low areas are highlighted—then what? The document just moves on to the next section without providing further context. The methodology seems to be missing the next steps or even a summary to simply relay how this information can be used and how it should be used in the context of SeBD.	Section 4 could benefit from a summary detailing how to compile the information being developed in Sections 4.2 and 4.3. They are two independent tables, so what are the recommended next steps? How should this information be used in the context of SeBD? Should the tables be updated once design changes are made until everything is green?

#	Category	Observation	Notes	Suggested resolution
19	Technical	Incorrect use of the term “risk”	Many tables specify “risk consequences,” but risk is a frequency or probability multiplied by a consequence. For example, tables such as “Summary of molten salt reactor (MSR) risk consequence rankings for various sources.” are purely consequence estimates. Risk cannot be derived from these tables and should be caveated and stated in the report.	In all tables, replace “risk consequence” with “consequence,” and then include an assumptions section stating that consequence-oriented approaches are not equivalent to risk but can inform decision-making in the absence of quantitative estimates for probability or frequency.
20	Technical	Radar plots	What value do radar plots provide the reader or INS stakeholder? What new information is gleaned from these plots? The radar plots generate more confusion than value in their current state. The plots are all equally spaced; does that mean they are all equally ranked? What is being communicated, and what is the takeaway here?	Either remove the radar plots, present a new benefit, or define how these points are intended to be used when interpreting the results.
21	Technical	Required correction	On page 118, a statement regarding Vogtle 3 reads “It is the first reactor to be constructed and operational in the United States in over 30 years.” This is not quite true. Watts Bar 2, while partially constructed in the 1980s, came online in 2016. If this is ignored, Watts Bar 1, which came online in 1996, would have been the second most recent.	Either delete the sentence or rephrase it, as Watts Bar 1 came online 27 years ago, and Watts Bar 2 was finished and brought online 7 years ago. It would be more accurate to say that “it is the first new reactor design to be licensed in the United States in more than 30 years.”
22	Technical	Long-term storage	The authors have excluded long-term fuel storage on site and/or the potential introduction of on-site reprocessing with AR technologies to focus on the technology itself. Both long-term on-site storage and on-site reprocessing options can introduce additional safety and security risks and may leave the reader questioning how to evaluate and incorporate those risks in a comprehensive security assessment.	Because there are no suitable long-term storage solutions, if possible, the authors should state that the risks associated with these activities are planned to be addressed in the future, and point the reader to existing documentation that addresses these scenarios. This stands out as a gap that still needs to be addressed, and no resources are readily available within the document.

#	Category	Observation	Notes	Suggested resolution
23	Technical	Category ranking criteria	Rankings are mostly based on SME opinions except for the radiation category, which has well-defined criteria. The methodology could benefit from better-defined criteria to support the ranking so that it can be applied with consistency. As written, it is not clear how the ranking presented in the paper was developed.	It is recommended that the ranking criteria be better defined to clearly differentiate between categories (high, medium, low). Justification should be included for the rankings presented for each technology in Section 5/Appendix A, e.g.: "This is high or low because it is [insert justification here]." As written, it is difficult to follow the logic, and the review team's SMEs disagreed with some of the rankings in the report. For example, the primary transport system for heat removal for advanced light water reactors (ALWRs) and large light-water reactors (LLWRs) was labeled as *low* for the safety function. The review team debated whether it should be high, but there was not enough information to justify one conclusion or the other. Otherwise, ranking criteria and justification for the rankings presented should also be included; using the current approach is not repeatable.
24	Technical	Summary-level ranking criteria	The roll-up of the ranking criteria is not defined for Table 4-1 and similar tables regarding SSC importance and security vulnerability. For example, in Table 4-4, line 1, SSC importance subcategories were ranked as *low*, *high*, *high*, and *none* – with the overall rank as *low*. Line two for SSC importance is *high*, *none*, *medium*, *none*, with an overall rank as *high*. This is confusing, difficult to follow, and propagated throughout the document in Section 5 and Appendix A.	In the interest of consistent application and repeatable results, a formula should be defined for use in compiling summary-level rankings.
25	Technical	Methodology concerns	In general, the security risk method is not easily applied in practice. A review team member tried to apply the method to the Westinghouse AP1000 design at a high level but found the method could not easily be completed and would require more information.	Have the authors tried to apply this methodology to some of the INL test reactors? Consider including a pilot study, possibly for the Marvel microreactor. Do the methods work? Are the results as expected? Could they be publicly released in a document like this? These questions point back to the initial questions regarding the level of sensitivity of this document.

#	Category	Observation	Notes	Suggested resolution
26	Technical	Methodology concerns	The core dispersibility measures do not account for the flow path of the reactor coolant system (RCS) outside of the containment vessel. Interfacing system loss of coolant accidents (ISLOCAs), steam generator tube rupture (SGTR, like Ginna) and spent fuel pool (SFP) boil off use high energy (decay heat, pressure) to release.	The authors should review the dispersibility scoring and criteria and revise carefully as needed.
27	Technical	Methodology concerns	It is confusing how the document relates Table 8-X (Appendix) to the Table 5-X (Section 5). For example, MSR security rankings are developed in Table 8-1 and summarized in Table 5-3. Section 5 never actually points to the Appendix (Section 8) for the additional detail. Additionally, the rankings in Section 8 have no justification regarding why they are high, medium, or low.	Please provide a justification for each choice of result. Given the same methodology, a different expert could choose a different result. The methodology is not consistent and not repeatable.
28	Editorial	Spelling and grammatical errors	The document needs to be scrubbed for spelling and grammatical errors.	It is recommended that a technical editor review the final document.
29	Editorial	Document layout	Including the list of references in each section gives the appearance that the document was assembled in pieces and is not very congruent. Additionally, having so many sections of references clutters the table of contents and breaks up the flow and readability of the document.	It is recommended that references be re-numbered and summarized in a single section at the end of the document.
30	Editorial	Abbreviation callout	When indefinite articles (i.e., a, and an) are used before abbreviations, the authors should consider the pronunciation of the first phonetic sound of the abbreviation. For example, “a SMR” is incorrect and must be changed to “an SMR.” The choice of *a* vs. *an* is based on the pronunciation of the abbreviation, not the first letter in the abbreviation.	Update document language throughout.