A Project to Encourage the Early Integration of Safety Assessment into the Design, License, and Build Process of Nuclear Power Plants – Status Report

Steve Krahn*[a], Brandon Chisholm[a], and Andrew Sowder[b]
[a] Vanderbilt University, Nashville, TN, USA
[b] Electric Power Research Institute (EPRI), Charlotte, NC, USA

Abstract: This paper discusses a project presently underway to develop a process for integrating the design and safety analysis of commercial nuclear reactors, using a structured, incremental and iterative approach that involves the phased development of preliminary safety analyses, integration of the safety analysis results into concurrent design efforts, and support towards the development of a probabilistic risk assessment (PRA). The project is sponsored by the Electric Power Research Institute (EPRI), and involves participation from organizations in academia and in the nuclear industry. Safety assessment (including PRA) is a key activity of EPRI manifested by its development of safety assessment tools for use by utilities. The approach under development aligns with existing practice and ongoing enhancement activities including: the ASME non-LWR PRA Standard, the draft ANS Risk-Informed, Performance-Based (RIPB) Design Standard 30.1, the Department of Energy's "Integrating Safety into Design" approach, and the industry-led Licensing Modernization Project.

Keywords: Process Hazard Analysis (PHA), PRA, safety-in-design, non-LWRs, risk-informed methods

1. INTRODUCTION TO THE PHA TO PRA PROJECT

Integration of appropriate safety and risk assessment methods into the design process for advanced nuclear reactors can provide valuable insights and feedback early in the process–when changes are less costly. Qualitative and semi-quantitative Process Hazard Analysis (PHA) methodologies are considered to be well-suited for such applications, and such studies can generate outputs that readily support the development of more quantitative models used to estimate risk. Also, use of PHA methods in this context is consistent with approaches endorsed domestically by the US Nuclear Regulatory Commission (NRC) [1] and the draft ASME/ANS Probabilistic Risk Assessment (PRA) Standard for Advanced Non-Light Water Reactor (LWR) Nuclear Power Plants [2]. Furthermore, this approach is also consistent with international safety-in-design approaches, such as the Generation IV International Forum's Integrated Safety Assessment Methodology [3], and the safety assessment approach suggested by the International Atomic Energy Agency [4]. Developers can benefit from the early use of safety assessment in order to start building a safety assessment approach needed for a reactor design as early as possible, since spreading the safety assessment cost over the design development process can lower the financial burden at later stages of reactor design [5].

The six Generation IV advanced reactor systems, as defined by the Generation IV International Forum (GIF), include the gas-cooled fast reactor (GFR), lead-cooled fast reactor (LFR), molten salt reactor (MSR), sodium-cooled fast reactor (SFR), supercritical-water-cooled reactor (SCWR), and very-high temperature reactor (VHTR) [6]. In addition to these top-level reactor technologies there are a variety of advanced non-LWR designs under development involving different selections for reactor fuels, coolants, moderators, and differing heat transport system designs. Due to the variation amongst the design details and operating conditions in these reactor designs, the hazard profile associated with each of these technologies is different, and the most risk-significant accidents for a given reactor type may be mitigated by a fundamental design feature of another. For example, even between specific MSR designs, there is

*Email address: steve.krahn@vanderbilt.edu

significant variability amongst the fuel material, chemistry, neutron spectrum, and system geometry [7]. Each of these design decisions can affect the frequency and consequences associated with a given event sequence and also produce event sequences that are unique to the reactor design. The NRC has expressed the desire to adopt a uniform technology inclusive approach when considering how to develop a method to review and license advanced reactors [1]. In order to allow for the same safety assessment approach to be beneficial to the most stakeholders, a flexible, technology neutral approach to identify hazards and assess risk in the system is needed.

Another stakeholder that could benefit from the further definition of a safety assessment approach for advanced reactor designs is the regulator that oversees the safety and operation of commercial nuclear reactors. The NRC has identified the need to develop the ability to review non-LWR technologies and to identify and resolve technology-inclusive policy issues that impact safety and regulatory reviews of non-LWR nuclear power plants [8]. Ongoing nuclear electricity generation industry-led initiatives look to work with the NRC to construct a relationship that is beneficial to both parties [9]. Conversations involving developers and regulators regarding the safety assessment approach for advanced reactors could help to reduce the uncertainty surrounding these reactor designs for both sides.

Many of the present nuclear safety requirements that the NRC has promulgated, and therefore, that reactor developers use as a basis for design, are based on deterministic and prescriptive requirements that were developed early in the life of the commercial nuclear industry [10, 11]. As a result, the set of event sequences that regulators, designers and safety analysts consider to be risk-significant are based upon the designs of commercial reactor designs with significant industry experience, namely Light Water Reactors (LWRs) [12]. Because the designs of advanced nuclear reactors can differ substantially from that of LWRs, it is possible that some of the LWR event sequences do not apply to these other reactor types and that the most risk-significant event sequences may not be covered by those evaluated for LWR designs. If the applicable hazards of a reactor design can be identified, and the risk significance assessed systematically at an early stage of design, the analysis can lead to design decisions that can help mitigate the risk of the most risk-significant accident scenarios. A more comprehensive and risk-informed approach for investigating the risk-significant occurrences will help to identify those accidents that should be of greatest priority to the designers of advanced reactors, to assist in verifying that the reactor design will perform the anticipated mission and meet public health risk safety goals.

The PHA to PRA (P2P) Project is intended to develop and demonstrate an approach that allows designers of an advanced nuclear reactor to analyze their design, incorporate safety insights into systems design, and incrementally build the safety case for their design. The project plan was developed using ideas and insights from subject matter experts in reactor design, hazard analysis, PRA, RIPB licensing, and affiliated domains; it is elaborating and documenting best practices used to integrate analytical results from early design stage safety analysis (e.g., process hazard analysis or PHA) into design and, subsequently, into PRA. The first deliverable of the project is the initial draft of a reference document, or "Body of Knowledge," that delineates best practices for bridging the gap from early-design-stage safety analysis to a PRA. Other significant features include coordination with the development of ANS draft standard on RIPB design (ANS 30.1), followed by case and pilot studies (discussed in section 1.2, below) to apply the developed methodology to an advanced reactor design.

1.1. Brief PHA Overview

Not all readers may be equally familiar with PHA. PHA methods for safety analysis were developed by the chemical process industry in the late 1960s and 1970s in response to accidents and refined into a technical guide after the 1984 toxic gas release from a pesticide plant in Bhopal, India; this work was done by the Center for Chemical Process Safety (CCPS), an applied research group within the American Institute of Chemical Engineers (AIChE) [13]. The CCPS describes several PHA methodologies that are

applicable for assessment of hazardous processes and facilities -- in varying stages of design and operations; these methods are referenced by both NRC [14] and DOE [15] for hazard analysis of new and modified nuclear facilities and processes. The six methodologies are listed below:

- Checklist Analysis
- What-If Analysis
- Checklist/What-If (Combined) Analysis
- Hazard and Operability (HAZOP) Analysis
- Failure Mode and Effects Analysis (FMEA)
- Fault Tree Analysis

Choosing among these industry-standard options to evaluate safety in a design, described in detail in [13], is based on the design information available for the evaluation, as well as the intended use of the results. In an EPRI analysis of one MSR design, the Liquid Fluoride Thorium Reactor (LFTR), the "What If" approach was chosen due to the limited design information available and the short time period available for the study [16]. However, the HAZOP approach has been chosen for the PHA of the Molten Salt Reactor Experiment (MSRE) in this project, since the safety analysis efforts are intended to eventually support PRA work, and since more detailed design information is available. Recent hazard and safety studies have been conducted on several MSR designs (for example, [17-19]); these studies will be helpful in performing the evaluations of the MSRE envisioned in Phase 2 of this project, discussed in Section 1.2.2 below.

HAZOP is recognized as a method that provides sufficiently detailed results to directly support PRA efforts, as described in the ASME/ANS PRA Standard for Advanced non-LWRs [2]; for example, HAZOP can be used for the task of identifying design specific initiating events. Additionally, one of the technical requirements in the PRA standard for non-LWRs (based on a similar requirement in the PRA Standard for operating LWR plants [20]) specifies that for each source of radioactive material potentially significant mechanisms by which this material could be mobilized to escape its initial confinement must be identified. The standard notes that FMEA, HAZOP, Master Logic Diagram (MLD), or equivalent methods are to be used for this purpose.

In this project, broader applications of PHA methods are being investigated to support the incremental early design stage development of PRA models, especially for new reactor technologies, and designs within each technology, that do not currently benefit from prior PRA development. Among some advanced non-LWR concepts currently in development, there is a history of PRA development; for example, High Temperature Gas-Cooled Reactors (HTGRs) and Sodium Cooled Fast Reactors (SFRs). Even for HTGRs and SFRs, the design-specific hazard information provided in a PHA had to be developed as a pre-requisite to developing those PRAs. On the other hand, for the family of MSRs, there is little PRA legacy to build on [19]. For this reason the initial investigation (below) of using PHA methods to support initial PRA model development is focused on MSRs, with specific focus on the Molten Salt Reactor Experiment (MSRE).

This is not to say that evaluation of the PHA to PRA transition should be limited to MSRs. Indeed, PHA techniques have also been useful to support the design of other nuclear power plants. HAZOP techniques, for example, were used to guide the development of control systems and control setpoint settings for the PBMR project in South Africa [21]. Further, the Licensing Modernization Project White Paper on PRA development recommends introduction of the PRA development early in the design and before the completion of the conceptual design [22]. The purpose is to incorporate risk insights into the initial design rather than waiting to back-fit them in a less cost effective manner after the reactor safety design approach has been formulated. Given that PHA has useful applications to support design development, it makes

sense to consider the introduction of PHA early in the design to both support the design and to provide structure to the initial development of a PRA for the advanced non-LWR technologies and designs.

1.2. Project Goals and Objectives

The value of this project derives from the collection, structuring, and demonstration of industry-standard practices that support an incremental step-wise approach to the integration of safety analyses with design efforts; therefore, the schedule and scope uncertainties with whether safety goals will be achieved can potentially be reduced. Additionally, these practices allow for the maximum leverage of investment in design over the entire lifecycle and early identification of unaddressed gaps and risks. The work in this project is also intended to be consistent with industry-led efforts to develop a more risk-informed and performance based licensing framework, as discussed in Section 1, above. Early and meaningful progress on this initiative should provide tangible benefits for many in the advanced reactor community, as they are currently facing the challenge of building a safety case for their designs in parallel with maturing those same designs.

In order to finalize both the scope for the project and the technical sequence of technical work, EPRI held a workshop at Vanderbilt University, July 17-18, 2017. The objective was to gather the ideas and insights from subject matter experts in reactor design, hazard analysis, PRA, risk-informed performance based licensing, and other affiliated domains, in order to inform and shape the initiation of the P2P Project. The first day of the workshop included a number of background presentations, with the first providing an overview and the context for the project and the remaining sessions addressing related technical subjects, including: an introduction to process hazard analysis; perspective on PRA in operating LWRs; the development and piloting of the ASME non-LWR PRA standard [2]; development of an ANS standard on risk-informed, performance based design [23]; an update on the Southern Company-led licensing modernization project [22]; an historical perspective on the evaluation and licensing of non-light water reactors; insights from licensing basis event identification case study performed by Vanderbilt and Oak Ridge National Laboratory (ORNL) [24]; an illustrative non-LWR nuclear application of PRA; and a utility perspective of customer expectations for the P2P Project. These sessions provided background and set the stage for a panel discussion and open dialogue on the P2P project scope and schedule the next day. A draft report of the proceedings, including conclusions regarding P2P scope and schedule (reflected below), was circulated for comment among the workshop attendees, prior to being finalized [5]. The project is intended to:

- Assembly a "Body of Knowledge" (BoK) on PHA and PRA application relevant for a progressively refined approach for integrating safety assessment into a “design-license-build-operate” process model for advanced reactor designs;
- Develop and describe a methodology for incrementally applying PHA in a manner that provides a smooth transition to PRA methods and supports a design-license-build-operate lifecycle for advanced reactor designs;
- Demonstrate of the application of a transition from PHA to PRA via a case study;
- Support the demonstration of the application and utility of PHA to PRA via a pilot application by an advanced reactor developer; and

The following subsections highlight how each of these project phases is structured to best benefit the designers, regulators, and customers of advanced reactor designs.

1.2.1. Phase 1 – Development of a BoK and Draft Methodology

The first phase of the P2P Project has consisted of a broad-based literature review to collect a BoK in the relevant subject matter and develop a draft methodology and approach. This phase:

- captures the wealth of history on safety assessment of reactor designs from which insights can be drawn;
- documents a comprehensive set of industry standards that supports the incremental development of reactor safety analysis and how the use of such an approach can help improve advanced reactor designs;
- documents examples from the nuclear industry and other industries for which the process has resulted in a safer or more economical design;
- explains how PHA can be used beyond safety analysis, such as identifying functional or performance objectives based on assumptions made during the analysis; and
- based on the above work, documents a draft methodology to incrementally build a safety analysis and describe its use in design maturation.

1.2.2 Phase 2 – Case Study

The second phase of the P2P Project will be a case study using the draft methodology and BoK reference material developed during Phase 1, to investigate specific systems or subsystems or even the design of a test facility. To maximize the benefit of this phase, the case study efforts will:

- Rely on publicly available information to select a system or systems to analyze that will be informative to a large number of interested parties, and
- Include engagement with non-LWR developers and other RIPB technical development efforts (e.g., Ref. 22 and 23) in anticipation of Phase 3, in which specific designs will be examined. The following systems have been proposed:
  - Off-gas systems
  - Pebble sorting systems
  - Online refueling systems

One set of insights that will be particularly important from this phase of the project pertains to the value added from the design insights identified as a result of the case study.

1.2.3. Phase 3 – Pilot with One or More Advanced Reactor Developers

The third phase of the P2P Project will lead to the development of the capstone report, which is intended to document the pilot study of systems important to an advanced reactor design team (and ideally of importance to the class of reactors which the particular design represents) using the methodology developed in Phase 1 and refined in Phase 2. This pilot study will be aligned with the resources, needs, and priorities of the pilot participants. Because specific design information will be involved in this phase of the project, it will be necessary to emphasize proper information control, export control, and safeguard and security practices.

The capstone report will document the as-developed methodology as well as useful insights from the experience obtained in Phases 2 and 3. This product should be of use to the entire community, and the goal is that the report (to be published in early 2019) will serve as a useful communication tool to facilitate use of safety analyses during early stages and throughout the design process for advanced reactors.

2. PROGRESS ON PHA TO PRA BODY OF KNOWLEDGE

The concept of a “body of knowledge” is not new. It is a mechanism that has been developed and refined by a number of professional groups to document accepted best practices in a field of technical endeavor; it has been used in the fields of: systems engineering, software engineering, project management and environmental engineering. The purpose of a BoK is to provide a widely accepted baseline of technical knowledge in a discipline. The documentation of such a baseline is intended to strengthen the mutual understanding of available best practices in the discipline. To provide a foundation for the desired mutual

understanding, a BoK provides a guide to the body of knowledge in a discipline; it is not an attempt to capture that knowledge directly. Thus, the BoK provides references to more detailed sources of knowledge, all of which are intended to be generally available to an interested practitioner (no proprietary information is referenced, but not all referenced material is free—for example, some books or standards may have to be purchased). The criterion for including a source is that the authors believe it offers the best generally available information on a particular subject.

A preliminary draft of the BoK concerning transitioning from PHA to PRA has been prepared. It was developed by a team of six (6) practitioners brought together by EPRI for this specific task. As a team they possess more than 150 years of experience in nuclear, chemical process and high-hazard systems safety analysis and design. The content for the BoK was developed incrementally over the space of about one year. The development process started with the team identifying references pertinent to the area of practice. These lists of references, along with short summaries of the major references, were compiled and circulated to the full team for comment and revision. Once the list of references was fairly stable, a preliminary outline of the knowledge areas represented by the compiled reference list was developed; the references were then sorted into the most appropriate knowledge area. From this compilation and sorting effort an initial outline for the BoK was developed, circulated for comment, and revised as necessary. After agreement was reached on the outline, writing assignments were established to draft the sections of the BoK -- based upon a set of format and content expectations. The knowledge areas addressed in the initial report published by EPRI [25] include:

1. Introduction (support for the “safety in design” approach);
2. Systems Engineering;
3. PHA and early-stage safety analysis;
4. Event sequence diagrams, event trees, and fault tree analysis;
5. Data collection, analysis, and handling of uncertainties;
6. Operations/internal events PRA;
7. Prior advanced reactor PRA projects; and
8. General/miscellaneous references

The objective of the BoK, when completed, is to introduce the reader to industry-standard tools that have been developed and used in the chemical process, aerospace and nuclear industries for early design stage safety analysis. These tools include PHA, along with tools for developing initial PRA models, such as event trees and fault trees, for advanced non-LWRs–in combination with some of the tools currently used to develop PRAs for LWRs. The references for each knowledge area summarized in this BoK are listed at the end of each subsection for easy and ready access to the reader. In each knowledge area, the following information is presented: (1) background discussion on the knowledge area, in general, (2) technical description of each major reference, and (3) within each sub-section an evaluation of the content of each reference that pertinent to the subject of PHA to PRA transition (identified as “noteworthy content”). It is anticipated that the structure and content will benefit from wider industry review and comment associated with the report that contains and discusses the BoK.

3. PROGRESS ON PHA TO PRA METHODOLOGY DEVELOPMENT AND DEMONSTRATION

3.1. PHA to PRA Methodology Development Insights

A quantitative PRA will ultimately be needed for any nuclear reactor for two reasons. First, it is a *de facto* component of a license to build a test, demonstration, or commercial reactor. Second, it provides focus and structure to the reactor development and design effort in terms of identifying necessary failure mechanisms and mitigating safety features. However, the input to a complete PRA requires the results of a

relatively mature reactor development and design program. While having the results of a PRA at the outset of the process for developing and designing a new reactor concept would be ideal, the reality is that the detailed information (and likely the resources) necessary to perform a complete PRA are not available in the early development stages. The reactor design is often no more than a piece of paper containing a summary-level flowsheet with major components in the primary loop and postulated temperatures and pressures based on literature data. As reactor development and design proceed, the additional details necessary to inform a PRA gradually emerge, supporting a substantially complete PRA in the later development stages. Nevertheless, it is important that the fundamental inputs to a PRA, such as the hazards present in the reactor concept and features that mitigate the hazards, be qualitatively identified at the earliest stages of reactor concept maturation.

The foregoing reality leads to the need to identify and use an approach to qualitatively evaluate hazards and mitigating features in any new reactor concept to provide focus for early reactor development efforts and to inform evolving reactor design and alternative assessment studies. Such an approach should not only meet this need but should do so in a way that produces information that is directly useful in developing increasingly detailed and quantitative PRAs for the reactor concept. The purpose of this section is to discuss a methodology that includes an appropriate qualitative evaluation process for identifying hazards and mitigating features in new reactor concepts and how the resulting information then flows into an evolving PRA. The relationship of the PHA results to the generic information needs for a PRA is shown in Figure 1.

During recent PHA studies of MSR systems [26, 27], it was found that comprehensively documenting the unmitigated effects of a deviation – the coupling of a system parameter such as pressure and an upset condition such as “too high” – within a section was beneficial to the process of translating HAZOP results to the construction of event trees. Thus, time spent exhaustively brainstorming causes and effects of deviations during a HAZOP study helps to ensure “comprehensiveness” in hazard identification and evaluation. Similarly, systematically assessing the consequences of the deviation/cause combination at each section interface ensured that the event sequence could be fully analyzed using HAZOP results from multiple sections. Because the goal is to eventually construct quantitative fault trees to estimate the probability of event tree pivotal events and event sequences, it is also helpful to differentiate between automatic system responses and anticipated operator actions in response to system indications. This differentiation will aid in the incorporating estimates of human error within a PRA model. Finally, a key to performing a consistent PHA is ensuring that the effects of all deviations or equipment failures are analyzed using consistent assumptions and that these assumptions are documented during the evaluation [13].

In a PRA, event trees model potential event sequences that occur after an initiating event. Event Tree Analysis assumes that the initiating event occurs and then represents each success or failure to respond to the initiating event as a pivotal event. Each event sequence is a path through pivotal events with an associated end state and, when the event tree is quantified using the results from fault tree analysis (see below), the probability of occurrence. The deviations evaluated during the HAZOP study provide inputs to the identification of initiating events. The comprehensive identification of causes and consequences, for those deviations selected as initiating events, assists in laying out the branches of the event tree; information from several systems may be combined to fully structure the event tree. The modeling the response of safety systems, identified during the HAZOP, will assist in distinguishing end states.

The results of the HAZOP studies and FMEAs on an advanced reactor design are qualitative; however, these PHA results will next be used to create models that can then be quantified to estimate the risks (failure probability or frequency) for a reactor design. It is standard practice to model the progression of nuclear reactor accidents and the end state resulting from event sequences using event trees. Some of the causes of deviations identified during the HAZOP study will represent initiating events in the event trees.

Additionally, the pivotal events that determine the different event sequences in event tree analysis will be captured as safety systems mitigating the deviation in the HAZOP results. Finally, the end state of the event sequence will be related to the consequences determined for relevant deviations during the PHA.

The frequency of each pivotal event in an event tree can be evaluated using fault tree analysis, if this information is not readily available from standard references (e.g., [28]). Fault tree analysis is a deductive approach that starts with the top-level event of concern and decomposes that event into sequences that contribute to its occurrence until the fundamental fault causes (known as "basic events") are identified. These basic events include equipment failures, human response errors, etc. Fault trees are quantified by inputting component reliability data and the frequency of the basic events, to estimate the probability of the top-level event. Fault trees model plant systems in detail, informing the PRA modeler of combinations of component failures that prevent the desired response to the initiating event. PRA modeling uses fault trees to represent the combination of individual component failures that will result in each pivotal event in an event tree.

The identification of the safety systems, those systems which the design depends on to monitor important parameters and provide alarms or protective actions, is a fundamental feature during HAZOP studies and FMEAs. This feature of these methods allows the qualitative review of which systems are identified most frequently, or are associated with mitigating more severe consequences—which provides an initial indication of systems that are important to safe and reliable operation of a system and the overall design. The consequences themselves are a primary output of the PHA, as they will assist in identifying and characterizing hazards. Also, as deviations and failure modes are being evaluated, the PHA team is required to document outstanding technical questions or analyses that are suggested by their assessments. These are generically referred to as "actions"; one of the concluding steps of the HAZOP study or the FMEA is to ensure that these actions are assigned to lead individuals in the project team for resolution.

As PHA results are used to develop event and fault tree models, the analyst gains an understanding of how the performance of each subsystem or component contributes to the progression of the event sequence from event trees. A deeper appreciation is developed of the interaction between subsystems and components in accomplishing the anticipated system function, along with the combination of responses that lead to varying levels of system failure can be obtained by developing the fault tree logic.

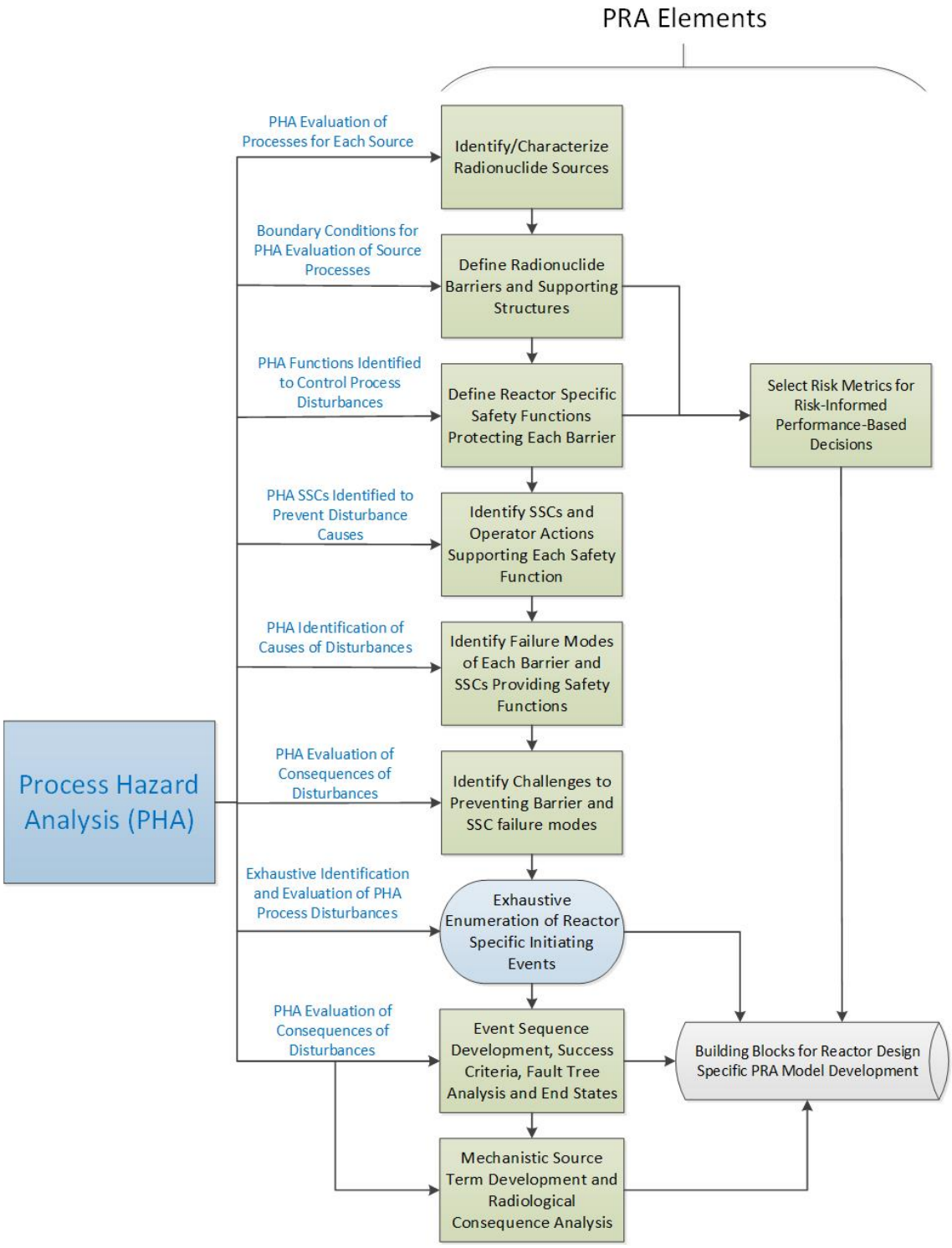

Figure 1: Conceptual Model of a PHA that Supports the Building Blocks of a PRA Model

3.2. PHA to PRA Methodology Demonstration

To provide an initial demonstration of the draft methodology for transitioning from PHA to PRA, a case study will be performed. To select an advanced non-LWR design to evaluate, the team took into consideration the fact that PRAs have been performed in the past on liquid-metal fast reactors and high-temperature gas reactors. Therefore, it was decided that it would be most beneficial to perform the case study evaluation on a different advanced reactor concept: a molten salt reactor (MSR). Many current MSR designs have published high-level descriptions of their designs but detailed design information is either proprietary or not yet developed. This led the team to assess the potential use of the Molten Salt Reactor Experiment (MSRE), operated by the Oak Ridge National Laboratory from 1965-1969. The MSRE does not have a PRA, or safety analysis done consistent with current standards. However, during a joint ORNL-Vanderbilt University project in 2017 [24], it was determined that there was sufficient design information available to support a PHA, and subsequent event and fault tree analyses that constitute core inputs to a PRA. The kick-off meeting for this case study was conducted in June 2018. The MSRE case study will be pursued as follows:

- Pre-Hazard Operability (HAZOP) Work/System Characterization
    - Functionally decompose the MSRE for the HAZOP study.
    - Identification of MSRE-relevant phenomena (system parameters) to consider during hazard assessment, along with the rationale for their selection.
    - Development of a preliminary risk metric (i.e. the conceptual equivalent of "core damage frequency" in a LWR system) that could be applied for the MSRE risk assessment.
- MSRE HAZOP Study
    - Use the HAZOP process to systematically evaluate the MSRE system sections, developed in the functional decomposition above. At least three separate sections will be studied, with these functional sections pertaining to the main sources of radioactive inventory in the MSRE.
    - Identification and documentation of significant system deviations (e.g., Anticipated Operating Occurrences), consequences, safety systems, and actions.
- Quantitative Risk Assessment of Selected Initiating Events
    - Development of fault and event tree analysis specific to MSRE to allow comparison of the frequency and consequence of event sequences.
    - Identification and documentation of the most significant system deviations.

The next phase of the project will involve using the appropriate industry-standard tools identified in the BoK and information from the case study above, as the basis for a pilot study of a PHA-to-PRA study for a yet-to-be-determined system important to an advanced reactor design team (and ideally of importance to the class of reactors which the particular design represents). This pilot study will be aligned with the resources, needs, and priorities of the reactor design team. Because specific design information will be involved in this phase of the project, proper information control will be required.

3.3 Summary

In this paper, we have provided an initial set of insights on how the early stage safety analyses of advanced reactor designs can be transitioned to the quantitative analysis and, ultimately PRA—that is, a draft methodology has been proposed. This has been done by presenting a simplified, three-step description of the methodology: (1) preparing for the PHA, which involves selecting a PHA methodology appropriate for the present stage of the system design and goals of the evaluation; (2) conducting the PHA

in accordance with available industry-standard guidelines and "keeping the end in mind" as the analysis unfolds; and (3) using tools such as event tree analysis and fault tree analysis to build the models of the system that are at the core of a PRA. Understanding of the transition of PHA results to event and fault tree analyses, and then an example PRA will be further developed during the case study and pilot study phase of this project. In particular, the case and pilot studies will include an effort to further document the details of the PHA-to-PRA process to provide insights for modifying the methodology and for future use.

4. CONCLUSION

This paper provides a status update on the first year of work on an EPRI project defining a process and methodology for transitioning from early, qualitative evaluations of system and overall design safety to comprehensive quantified assessments of risk that will support design refinement and the development of safety case for an advanced reactor concept. The project has been divided into three phases, of which the first phase, involved the development of a preliminary Body of Knowledge (BoK) for the subject matter area, and drafting of a methodology for conducting the analyses in a manner that is efficient and mutual supportive, have been covered in this paper.

Review of the references that make up the eight knowledge areas of the BoK supports the conclusion that there is sufficient, industry-standard guidance available for conducting the types of analyses that contribute to a qualitative understanding of the safe and effective operation of an advanced reactor design. These analytical tools include: HAZOP studies, Failure Modes and Effects Analysis (FMEA), Event Tree Analysis (ETA) and Fault Tree Analysis (FTA), discussed in more detail in this paper (among others that could be used); each of which was developed with an end in mind—other than direct support to PRA. With that said, there are explicit contributions that each tool makes to laying the foundation for PRA and it is important to ensure that they are pursued consistent with expectations for PRA information sources, if a PRA is planned. At the end of the previous section a diagram that aids in visualizing how the technical content of PHA tools (such as HAZOP, FMEA, ETA and FTA) support the development of PRAs was presented. What remained was initial efforts to propose an arrangement for integrating the performance and insights from these reviews. In developing this arrangement, it was assumed that previous hazard assessments had not been performed—thus the analyst was starting with a "clean slate." The next step was an attempt to logically arrange the PHA tools from methods intended to be comprehensive, but perhaps forgo a level of detail, to those that perhaps focus on developing more specific insights.

The proposed arrangement or structure is depicted in Figure 2, where (1) HAZOP serves the role of "moderately detailed PHA" in this project; (2) FMEA acts as a "more detailed PHA" tool, for example, in the instance where sub-systems are proposed that have no prior analysis; the results of the FMEA can then inform, with component reliability data, FTA -- that provides quantitative information on failure rates -- which is one feed to quantitative ETA and PRA; (3) the deviations identified and analyzed in the HAZOP study support event sequence elaboration as an input to development of qualitative event trees; (4) summary review of causes and consequences identified in the HAZOP supports the determination of those consequences for which quantitative estimation is to be pursued, which contributes information needed for quantitative ETA; and (5) a relevant risk metric can serve as a tool to evaluate the outcomes in the quantitative ETAs and ultimately the PRA. This overall structure is reflected in the methodology discussed in the previous section and will be used in the case and pilot studies.

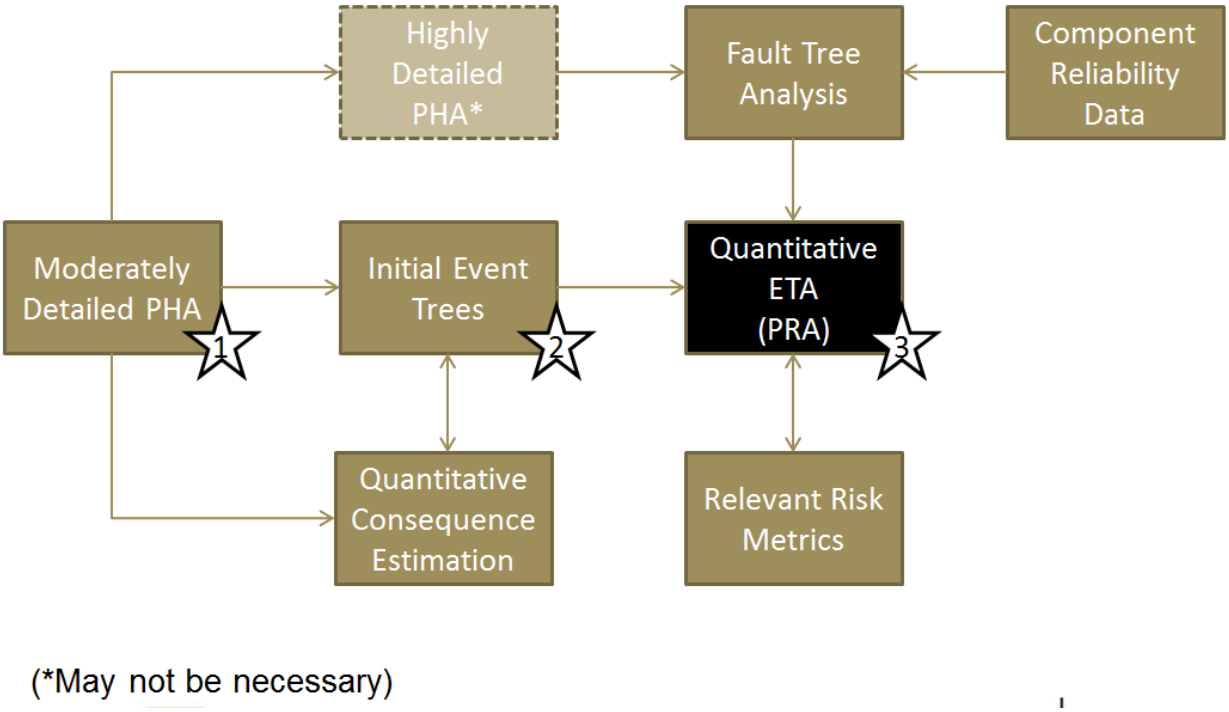

Figure 2: Transition from PHA to PRA – Overall Process Flow

Acknowledgements

The authors would like to acknowledge EPRI for partial sponsorship of this research. The authors would also like to acknowledge the assistance of Oak Ridge National Laboratory and Southern Company Services in this project. This material is based upon work partially supported under a Department of Energy, Office of Nuclear Energy, Integrated University Program Graduate Fellowship.

References

[1] NRC, "Policy statement on the regulation of advanced reactors."*Final Policy Statement, October* 7 (2008): 4-2.

[2] ASME/ANS, “Standard for Probabilistic Risk Assessment for Advanced Non-LWR Nuclear Power Plant Applications,” RA-S-1.4-2013, 2013.

[3] GIF Risk and Safety Working Group (RSWG), “An Integrated Safety Assessment Methodology (ISAM) for Generation IV Nuclear Systems.” Version 1.1, June 2011.

[4] International Atomic Energy Agency (IAEA), “Procedures for conducting probabilistic safety assessment for non-reactor nuclear facilities.” 2002: Vienna, Austria.

[5] EPRI, “Program on Technology Innovation: EPRI Workshop on Process Hazard Analysis to Probabilistic Risk Assessment for Advanced Reactors Proceedings,” Vanderbilt University, Nashville, TN, July 18-19, 2017. 2017: Palo Alto, CA.

[6] GIF, “Technology Roadmap Update for Generation IV Nuclear Energy Systems.” 2014, OECD Nuclear Energy Agency.

[7] Dolan, T., *Molten Salt Reactors and Thorium Energy*. 2017, Woodhead Publishing.

[8] NRC, “SECY-18-0011: Advanced Reactor Program Status.” 2018.

[9] Cowan, P., “NEI Activities in Support of Advanced Non-Light Water Reactors.” 2016, Nuclear Energy Institute: Washington, D.C.

[10] NRC, “WASH-1400, The Reactor Safety Study: The Introduction of Risk Assessment to the Regulation of Nuclear Reactors,” NUREG/KM-0010. 2016: Washington, DC, USA.

[11] Keller, W. and M. Modarres, “A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late Professor Norman Carl Rasmussen.” Reliability Engineering and System Safety, 2005. 89(3): p. 271-285.

[12] NRC, “NUREG-0800, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, LWR Edition.” March 2007: Washington, DC, USA.

[13] CCPS, *Guidelines for Hazard Evaluation Procedures*. Third Edition. American Institute of Chemical Engineers (AIChE). New York: John Wiley & Sons.

[14] NRC, “Integrated Safety Analysis: Why It Is Appropriate for Fuel Cycle Facilities,” Staff Report, 2013.

[15] US DOE, “DOE Standard on Development of Probabilistic Risk Assessments for Nuclear Safety Applications.” 2013

[16] EPRI, *Program on Technical Innovation: Technology Assessment of a Molten Salt Reactor Design.* Final Report, EPRI 3002005460, October 2015.

[17] Allen, T., et al. “Fluoride-Salt-Cooled, High-Temperature Reactor (FHR) Subsystems Definition, Functional Requirement Definition, and Licensing Basis Event (LBE) Identification White Paper.” Integrated Research Project Workshop, 2013.

[18] Qun, Y., et al. “Application of the Probability-Based Safety Analysis for the Reliability Evaluation of a Special Fuel Salt Release System Design in the Molten Salt Reactor.” ASME 25th International Conference on Nuclear Engineering, 2017.

[19] Uggenti, A.C., et al. “Preliminary functional safety assessment for molten salt fast reactors in the framework of the SAMOFAR project.” Abstract submitted to the International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA2017), Pittsburgh PA, USA. 2017.

[20] ASME, “Addenda to ASME/ANS RA-S–2008 Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications,” ASME/ANS-Ra-SB-2013, September 2013

[21] Joubert, J., N. Kohtz, and I. Coe. "South African Safety Assessment Framework for the Pebble Bed Modular Reactor." Fourth International Topical Meeting on High Temperature Reactor Technology. American Society of Mechanical Engineers, 2008.

[22] Southern Company, “Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors Probabilistic Risk Assessment Approach,” draft (June 2017).

[23] ANS. “Integrating Risk and Performance Objectives into New Reactor Nuclear Safety Designs.” ANS 30.1-201x (new standard under development).

[24] Chisholm, B., Flanagan, G., Krahn, S, Mays, G., “Licensing Basis Event Selection Case Study: The Molten Salt Reactor Experiment.” Paper presented at the ORNL MSR Workshop 2017, October 3-4, 2017, Oak Ridge, TN

[25] EPRI, *Process Hazard Analysis to Probabilistic Risk Assessment Project: Preliminary Body of Knowledge and Methodology*. Palo Alto, CA: 2018.

[26] Chisholm, B., Krahn, S., Marotta, P., Croff, A., “Preliminary Risk Assessment of a Generalized Molten Salt Reactor Off-Gas System”. Transactions of the American Nuclear Society, 2017. Vol. 117. pp 221-224.

[27] Chisholm, B., Krahn, S., Afzali, A., and Harvey, E. “Application of a Method to Estimate Risk in Advanced Nuclear Reactors: A Case Study on the Molten Salt Reactor Experiment.” accepted for

presentation at the Probabilistic Safety Assessment and Management Conference (PSAM 14), September 2018, Los Angeles, CA.

[28] CCPS, *Guidelines for Process Equipment Reliability Data, with Data Tables*, AIChE, 2010: John Wiley & Sons.