INL/EXT-20-59202

R&D Roadmap to Enhance Industry Legacy Probabilistic Risk Assessment Methods and Tools

Andrew Miller, Stephen Hess, and Curtis Smith

August 2020

U.S. Department of Energy Office of Nuclear Energy

INL/EXT-20-59202

R&D Roadmap to Enhance Industry Legacy Probabilistic Risk Assessment Methods and Tools

Andrew Miller[1]
Stephen Hess[1]
Curtis Smith[2]

August 2020

[1]Jensen Hughes
158 West Gay Street, Ste. 400
West Chester, PA 19380

[2]Idaho National Laboratory
2525 Freemont Avenue
Idaho Falls, Idaho 83415

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

EXECUTIVE SUMMARY

Probabilistic risk assessments (PRAs) are integral to nuclear power plant (NPP) operations, having tremendously benefitted the safety of the U.S. reactor fleet for decades. Insights obtained from the models have provided perspectives on a variety of applications, both at the plant and pertaining to the regulator. While these models are very useful, they are now being asked to represent and analyze aspects of the plant that were never envisioned by the initial PRA practitioners. Furthermore, heightened demands on the PRA models have led to increased computing power requirements. Additionally, as the complexity of the PRA models increased, the difficulty experienced by non-PRA experts in trying to understand these models, grasp the insights they provide, and effectively utilize that information has become problematic.

The need for research to address key issues regarding PRA tools and methods has never been greater. Although the nuclear power industry has largely been well-served by these tools and methods, the underlying science is dated, remaining mostly unchanged for over two decades. Newer tools and technologies are rapidly being developed to potentially address the challenges associated with legacy approaches to PRA. This document outlines key challenges identified by PRA practitioners and details R&D priorities for helping plan future resource investments.

CONTENTS

ACRONYMS

ATHEANA	A Technique for Human Event Analysis
AI	Artificial Intelligence
CAFTA	Computer-Aided Fault Tree Analysis System
CDF	Core Damage Frequency
CRM	Configuration Risk Management
EPRI	Electric Power Research Institute
FLEX	Diverse and Flexible Coping Strategy
FPRA	Fire Probabilistic Risk Assessment
GUI	Graphical User Interface
HEP	Human Event Probability
HFE	Human Failure Events
HRA	Human Reliability Analysis
IAEA	International Atomic Energy Agency
IE	Initiating Events
LERF	Large Early Release Frequency
MCUB	Minimum Cut Upper Bound
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
PRA	Probabilistic Risk Assessment
PRM	Phoenix Risk Monitor
RI	Risk-Informed
SAPHIRE	Systems Analysis Programs for Hands-on Integrated Reliability Evaluations
SDP	Significance Determination Process
SPRA	Seismic Probabilistic Risk Assessment
SSC	Structures, Systems, and Components
SPAR	Standardized Plant Analysis Risk
QA	Quality Assurance

1. Background

Probabilistic risk assessments (PRAs) in the nuclear power industry have tremendously benefitted the safe operation of the U.S. reactor fleet for decades. Insights obtained from these incredibly detailed models have afforded useful perspectives on everything from configuration control to maintenance to inter-system interactions. Plant PRA models are used extensively by both plant operators and regulatory personnel, and PRA technology has been instrumental for demonstrating the improvements to plant safety over time. For example, a recent study by the Electric Power Research Institute (EPRI) used industry data from required periodic updates of plant PRA models to show an order of magnitude reduction in the average core damage frequency (CDF) of plants over the previous 30 years of operations—in which the average plant capacity factor increased from ~70% to over 90% [1]. In the U.S., PRAs are fundamental to the regulatory infrastructure of the Reactor Oversight Process, particularly when used in the Significance Determination Process (SDP) for regulators to assess and classify the degree to which various events might impact plant safety [2]. Finally, for plant operators, PRA technologies are fundamental for meeting regulatory requirements while still improving plant operational efficiencies. Examples include:

- Fire protection programs [3]
- Maintenance rule (10CFR50.65) programs (including plant configuration risk management [CRM] programs for conducting online maintenance activities) [4]
- The Surveillance Frequency Control Program [5]
- Alternative treatment (10CFR50.69) programs [6]
- Risk-Managed Technical Specifications programs [7].

It should be noted that the last of these, Risk-Managed Technical Specifications programs, utilizes plant PRA and CRM models to evaluate and control the acceptable amount of time a plant's safety-related systems, structures, and components (SSCs) can remain out of service as part of the plant's technical specifications, thus necessitating that plant PRA models be queried and evaluated on a real-time basis as plant conditions change.

PRAs are so ingrained into plant operations that the models are now being asked to analyze aspects of the plant that were never envisioned by the initial PRA practitioners. Heightened demands on PRA models have led to increased demands for computing power. Increased model complexity generates expanded memory allocations and processing power requirements. Tradeoffs are sometimes made due to the lack of computing resources, and these almost always involve additional computational time. Such tradeoffs are not ideal, since, as was mentioned, PRA models now evaluate changing plant conditions in real-time. This means they must be capable of immediately identifying unexpected equipment failure and imparting knowledge of configuration risk to plant operators, who rely on this information to operate the plant safely. The same is true for PRA practitioners involved in model development, maintenance, analysis, and rollout. Increased complexity means reduced speed in everything from analyzing event combinations for dependency/criticality to quantifying multi-hazard models.

Additionally, with the increased complexity of plant PRA models, difficulties experienced by non-PRA experts (particularly plant operators and management personnel) in understanding these models, grasping the insights they generate, and effectively utilizing this information to support effective decision-

making has become increasingly problematic. The situation is now critical, given the technology's prevalence in supporting real-time operational decisions at the plant, as described above.

The need for research to address key issues in PRA software has never been greater. Although such software has long served the industry well, the technology for building, analyzing, and displaying PRA results has remained largely the same over the past decade. New tools and technologies are rapidly being developed, especially in the fields of machine learning and artificial intelligence (AI). These areas must be explored for potential benefits to the PRA and nuclear-power communities for as long as risk information continues to provide valuable insights for informed decision-making.

2. Issues and Challenges

2.1 Current Risk-Assessment Tool Issues

2.1.1 Quantification Speed and Efficiency

The single most discussed issue regarding current PRA software tools is the speed at which the models will quantify generating enough cut sets to deem the model "converged." Increased model complexity has expanded the required computing power and memory allocation necessary to evaluate and quantify the models. In some cases, these computational cost increases are exponential and difficult to mitigate with additional hardware alone. For example, models featuring millions of cut sets or many terms per cut set may exponentially boost the memory demand for performing the required calculations. Extremely long quantification times may lead to taxing the quantification engine, resulting in a long waiting period followed by quantification failure due to memory limitations.

This issue is most readily apparent in fire PRA (FPRA) models in which the number of fire scenarios and plant SSCs modeled are orders of magnitude larger than for typical internal-events models. An FPRA model is generally created by developing a common tree structure representing the SSCs at a nuclear power plant (NPP), then inserting events representative of a fire scenario in locations logically equivalent to the SSC(s) failed by the fire. These models have very large databases in order to represent the complex spatial interactions in NPPs by associated items such as fire zones, raceways, cables, components, and, ultimately, the location in the PRA model where the new events will be inserted. However, inserting all this information into the fault tree would yield models impossible to solve. Currently utilized PRA software analyzes these spatial relationships prior to placing new events into the fault trees, so only the scenario initiator is ultimately inserted in the location of the failed fault-tree element. This speeds up quantification but reduces the ability to determine which spatial relationships affected the plant. As a result, obtaining useful insights becomes labor- and time-intensive and, in certain applications (e.g., evaluating a plant event in the context of an SDP), places excessive demands on plant staff/management.

Even when employing this technique, quantification of FPRA models is considered unacceptably slow by industry practitioners. It can take as long as several days to produce a satisfactory result. Then, analysis and refinement of the model is still required, necessitating re-quantification to check the results of the modifications. Utilizing FPRA models has become commonplace in plant CRM programs and for operators or risk modelers who, for maintenance-planning purposes, rely on them for determining the relative risk of previously unanalyzed plant configurations. Slow quantification speeds can limit effective decision-making and delay the completion of maintenance activities.

2.1.2 Dependency Analysis for Human Reliability Analysis

Second only to quantification speed and efficiency in terms of importance, dependency analysis used in human reliability analysis (HRA) is a major hinderance to effective, efficient use of plant PRA models. The predominant tool currently used by industry for conducting dependency analysis is an EPRI product called the "HRA Calculator." It requires analyzing a cut-set file against HRA data to determine when individual events combine, gauge their dependency on each other, create combination events, assign an updated probability for each combination, and insert these new events into the cut sets. The process is cumbersome and time-consuming for large models. Due to substantial uncertainties in probabilities associated with—and outcomes arising from—human actions, this process is highly labor-intensive and inefficient. Additionally, the process must be updated and re-performed for even the most minor changes to the model, thereby contributing to additional costs. Once the analysis is complete, a recovery process is

employed—after the cut sets are generated—to find and replace individual events with combination events and new probabilities.

Two major issues are associated with dependency analysis, the first being the usefulness of the combination events created. In the current methodology, random counters are assigned to the combination events, thus reducing the chance of naming conflicts being introduced. However, this creates an issue when analysts attempt to identify particular events when reviewing model cut sets and interpreting the results. A more efficient and practical naming algorithm could assist practitioners in model review/interpretation by enhancing the predictability and transparency of the models.

The second issue associated with dependency analysis is the process of getting dependency results when modeling multiple human actions. This includes having to quantify the model with Human Event Probabilities (HEPs) set to an artificially high value (usually 0.1 or 1.0) to ensure that potential combinations of individual events do not "truncate out" prior to being fed into the HRA Calculator. This exacerbates the quantification speed issue, as quantification of more events above the truncation line takes longer and requires more memory. The process must also be repeated for each change to the model or underlying HRA data, resulting in inefficiencies such as those already described. Lastly, the recovery process defaults to removing the individual events from the cut sets and replacing them with the dependent event. An additional problem arises when a cut set is applied to the fault tree model to "browse" the results but the tree cannot correctly display the path followed to the top gate, as the dependent events do not exist in the tree.

2.1.3 Model Development, Maintenance, and Updates

A large challenge for the PRA industry is gathering enough manpower to fully complete PRA models with sufficient detail to provide valuable insights to plant operators. This goal is accomplished through periodic maintenance of and updates to existing models in order to add details, fix outstanding issues, and analyze new results from the updated model. The process is manual, labor-intensive, and prone to error due to human factors. One method that modelers employ to gather the most insights possible through the least amount of effort is to focus on key contributors to the overall answer and provide sufficient detail regarding the systems or plant operations in question. However, when risk applications such as SDPs arise, insufficiently detailed areas are uncovered, yielding potentially conservative results. In some cases, the given model cannot represent a particular failure of interest to the plant, so an application-specific model must be created. This takes time away from analysis and providing the plant staff (and management) with insights, leaving the PRA team scrambling to develop an appropriate representation of those conditions. An automated way of providing additional modeling details and validating that the model represents the intended design would benefit almost every day-to-day risk-related activity at the plant.

In addition to the model itself, manipulation of the model during risk applications is critical for providing the models with the right input files to make the quantification meaningful to the application. This is generally accomplished by utilizing "flag" settings that enable events to be manipulated in a text file so their value(s) or structure(s) can be changed prior to being sent to the quantification engine. Creating the flag settings for most applications (e.g., SDPs and risk-informed completion time calculations) is a manual process in which an engineer must review the model, manually locate the event or gate representing the equipment, and add it to a flag file using a special command format. Then, the practitioner must take that information and document the results. Once again, the process is time-consuming, inefficient, and prone to error. These processes would benefit from a method where existing mapping of events to SSCs to reduce the time spent searching for appropriate specific events, as well as an automated documentation process once the SSCs are selected for manipulation.

Current PRA tools require that many files work together to provide enough information for a quantification engine to perform its task. One such file is a database containing all the events and their failure probabilities. A large portion of the update process consists of taking raw failure data, updating them with the latest test results (since the last update), and converting them into new failure probabilities for key components. This process usually takes place outside the actual PRA software and must be imported into the database containing the event data. A streamlined software tool could reduce the time required, minimize error, and speed up the data updates—all within the PRA software itself.

2.1.4 Risk Aggregation

2.1.4.1 Multi-hazard Models

Risk aggregation of multi-hazard models continues to gain importance, with increasing levels of requirements being specified for many modern risk applications. This poses a challenge when combining certain external hazards with more traditional internal-events PRA models. Most internal-events models rely on the rare-events approximation when calculating the overall estimate for the top gate being quantified (e.g., CDF or large early release frequency [LERF]). In this methodology, the calculation assumes that the failure probability of each event is sufficiently low (e.g., 1E-2 or lower) and the success probability is relatively high (e.g., 0.99 [basically 1]). Decades of experience in using PRAs for internal events in which random failures of plant SSCs are assumed have proven this assumption to generally be appropriate, given the observed frequency of failures for nearly all SSCs included in plant PRA models. Therefore, when determining the probability of failure for an event, one can safely ignore evaluating and subtracting the cross product of the two terms, as they are both assumed to be greatly lower in value and, when multiplied together, the subtraction would not yield a significant reduction in the calculated probability.

For external events in which SSC fragilities are calculated (e.g., earthquake, high winds, external flooding), failure probabilities often have substantial values (e.g., 0.5 or 0.8). Therefore, the success probability cannot be assumed to be near 1.0, and the cross product of the two terms now becomes non-trivial but essential for an accurate risk estimate. For such conditions, calculating the mathematically correct probability of failure is possible for very simplistic or small models using the current suite of PRA tools, but a modern seismic PRA (SPRA)—as one example—will quickly run out of memory trying to store all the values to accurately calculate the probability without using the rare-events approximation.

As a result, industry created another approach/tool to estimate risk using cut set files more accurately. The tool factors out the initiators, utilizes binary-decision-diagram logic to calculate the true probability of failure of the cut sets for each initiator, then factors the initiators back in to generate a frequency-based estimate of risk. This solution is applicable to models that only represent one hazard (e.g., the SPRA-only model), but a multi-hazard one top model combines cut sets from all hazards into a single file. SPRA cut sets often drastically overestimate the risk from seismic events when utilizing the minimum cut upper bound (MCUB) estimation—in some cases being an order of magnitude higher than a "best estimate" of the risk. Despite such overestimation, SPRA cut sets may not individually contribute as much as fire-initiated cut sets, and this is where the software limitations become apparent. The EPRI Advanced Cut Set Upper Bound Estimator (ACUBE) software only allows users to specify the top N number of cut sets, and it starts from the top and works its way down. Given the complexity of multi-hazard one top models, available memory limits may be reached well before a sufficient amount of SPRA cut sets are processed and properly calculated, resulting in an overestimation of risk due to the non-processed SPRA cut sets.

2.1.4.2 Multi-Unit Sites

Current NPP PRA models estimate the risk to each individual NPP unit, independent of the other units located at the site. However, many NPPs feature the co-location of multiple units on a single plant site. As a result, an accident in one unit at the site can potentially impact the co-located units in several ways. First, an accident in one unit will impact the resources available to ensure that the remaining units at the site can be maintained in a safe condition (either operating or shutdown). Such resource limitations can relate either to using onsite personnel to respond to the accident or using plant SSCs designed to be shared among the multiple units. Note that use of personnel resources is mostly relevant to the early stages of accident response, before additional resources can be mobilized and arrive onsite. Second, for accidents initiated by a common external cause (such as seismic, flooding, or high-wind events), all units at the site will simultaneously become subject to the external hazard, simultaneously increasing the risks experienced by each unit. This situation was demonstrated during the Fukushima Daiichi accident, in which a single set of common initiators (seismic event and subsequent tsunami) led to severe core damage at multiple units at the plant site. To date, this limitation in PRA technology has not been addressed, though it is recognized by industry, regulators, and policy-makers. Recognition of this situation led the International Atomic Energy Agency (IAEA) to develop and publish technical guidance for NPPs to conduct PRAs at sites with multiple reactor units [8]. This proposed approach builds on existing single-unit PRA approaches in order to identify potential considerations for multi-unit PRAs, including the assessment of correlated hazards (e.g., high winds and flooding caused by storm surges) that could impact single units but are generally not included in single-unit PRA models. In an effort to apply this guidance, IAEA initiated a coordinated research effort to develop multi-unit PRAs across different power reactor designs in several participating countries. This effort was recently initiated and is expected to continue through 2022, with the following objectives [9]:

- Identify the main contributors for multi-unit risks from knowledge of single-unit risks.
- Develop a best-practice guidance document for conducting Level 1 and 2 multi-unit PRAs.
- Complete the benchmark exercises and document any lessons learned.

2.1.5 Analyzing Combinations of PRA Model Elements for Criticality

As mentioned in Section 2.1.2, dependency analysis is an important step in PRA model development. HRA already utilizes this technique as an integral part of the analysis, but another area of dependency is becoming more and more crucial to understanding plant and model interactions. In spatial analyses such as FPRA (or in assessing other externally induced hazards such as flooding and high winds), many plant SSCs can be impacted. However, not all the SSCs impacted are critical to satisfying the top gate. Recently developed tools are able to analyze FPRA spatial interactions and determine the criticality of an individual element such as a raceway or cable. Often, it is not a single element that proves critical, but a set of elements that could be protected to substantially reduce risk. Current PRA tools do not have a simple or effective way to identify these combinations of elements and/or determine the most important combinations for preserving computer hardware resources or reducing analysis time required to generate such a list.

This topic is becoming critical to the effective, efficient analyzation of FPRA models. Once a model is built, it is difficult to ascertain the key elements contributing to the overall risk estimate, due to tradeoffs among quantification speed, memory usage, and model transparency. Removing all the relationships from the fault tree reduces the quantification time and memory requirements but leaves out information for easily determining how the elements interact. Because external hazards other than earthquakes and (internal) fires are only just beginning to be incorporated into plant PRAs (i.e., so-called

"all-hazard" PRA models), this issue is anticipated to increase in significance over time. Therefore, a method for quickly analyzing combinations of elements tracked during post-processing software algorithms would greatly enhance PRA practitioners' ability to focus on model and plant improvements.

2.1.6 Uncertainty Analysis

Uncertainty analysis of PRA models is a necessary task, particularly for supporting risk-informed (RI) applications and regulatory interactions. However, it is often viewed by practitioners as just another checkbox to tick for model completion. Parametric uncertainty is generally determined by a software tool that applies a random sampling approach to values used in the PRA model, based on uncertainty distributions associated with these sampled events. The outcome is typically a log-normal-shaped curve due to assigning the individual events log-normal distributions. The point being that the act of performing parametric uncertainty analysis at the end of a model development cycle is entirely routine, with little to no new insights gained from the exercise.

While it would be difficult to apply any type of inverse assessment to PRA models due to the relative lack of failure data at NPPs, recent trends have indicated a desire to collect and process the data available from years of continued operations. Some components will not have as much reliability data as those tested regularly, and the tests may not reflect actual performance, due to their standby functions; however, all that can be taken into account when performing an updated analysis. Although methods exist to evaluate this historical performance, industry experience shows that such data collection/analysis is extremely labor-intensive and expensive, leading to the conclusion that this activity is not justifiable from a cost-benefit perspective. It is also believed that industry has extensive programs in place (e.g., the Maintenance Rule and aging management plans [for NPPs operating during periods of license extension]) to identify and correct degradations in SSC performance before they manifest as increases in the respective SSC failure rates used in the PRA models.

2.1.7 Communication of Risk Insights

The PRA community has always had a problem on its hands: NPPs are complex systems that interact with human operators, resulting in the need for nuisance modeling, results, and insights. This situation is further exacerbated by utilizing impossibly small numbers to represent the remote chance of multiple systems not working properly and operators failing to implement written procedures. Communicating PRA information to non-PRA practitioners has also been a challenge ever since the beginning of the industry.

To increase speed and efficiency, current PRA tools have sacrificed features that would enhance the general understanding of modeled results. This means that models often use cryptic shorthand to represent various SSCs and operator actions. Cut sets—the main output of the model—are long lists of event combinations that led to satisfying the quantified gate in the model. They are often the most overwhelming way for non-practitioners to view model results. Visualization of the results is relegated to pie/bar charts that use the same cryptic naming convention. Software tools often just allow for the basic elements to be included and have limited ability to provide better descriptions or update the names to something more intuitive.

Lastly, the basic computer visualization tools were invented decades ago and an upgrade to the types of visualizations needed for PRA is long overdue. New methods for displaying data (i.e., open-source libraries) include nodal diagrams, Sankey plots, and interactive updates to pie/bar charts. Data from PRA models are complex and unique in certain ways, but research could lead to methods of converting the data so they can be utilized in new charting options, or to the discovery that existing tools can display the data appropriately after a few minor adjustments. As a new generation of PRA engineers

prepares to replace the outgoing one, additional visualization capabilities could reduce the time required to become familiar with the models, boost the understanding of complex interactions, and allow more time to be spent prioritizing valuable plant modifications, thereby increasing nuclear safety as a whole.

2.1.8 Incorporating New PRA Technologies into Existing Models

The Risk-Informed Systems Analysis Pathway developed a simulation approach to risk analysis. This approach combines both probabilistic and mechanistic modeling (see Figure 1).

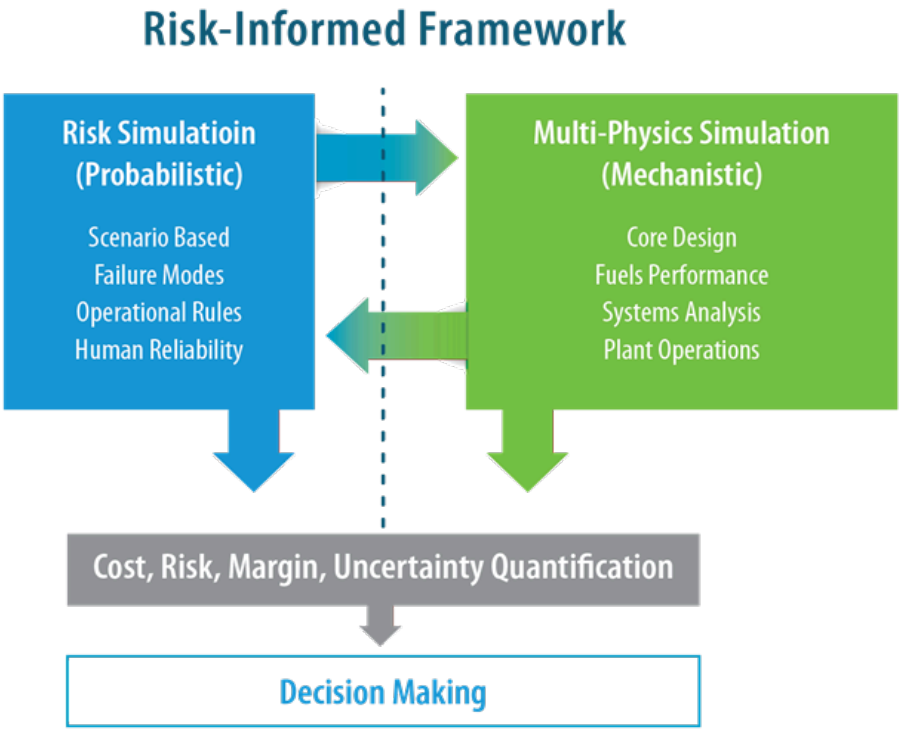

Figure 1. Types of analyses used in the Risk-Informed Systems Analysis Pathway.

The mechanics of conducting the simulation analysis, including a methodology for carrying out simulation-based studies of safety margin, follow these generic process steps:

1. Characterize the issue to be resolved in a way that explicitly scopes the modeling and analysis to be performed. Formulate an “issue space” describing the safety figures of merit to be analyzed.

2. Quantify the decision-maker and analyst’s state-of-knowledge (uncertainty) of the key variables and models relevant to the issue. For example, if long-term operation is a facet of the analysis, potential aging mechanisms that may degrade components should be included in the quantification.

3. Determine issue-specific, risk-based scenarios and accident timelines.

4. Represent plant operations probabilistically. For example, plant operational rules (e.g., operator procedures, technical specifications, and maintenance schedules) provide realism for scenario generation. Because numerous scenarios will be generated, plant and operator behaviors cannot be manually created as in current risk assessments using event- and fault-trees. In addition to the *expected* operator behavior (plant procedures), the probabilistic plant representation will account for the possibility of failures (see Figure 2).

5. Represent plant physics mechanistically. The plant system's level code will be used to develop distributions for the key plant process variables (i.e., loads) and the capacity to withstand those loads under the scenarios identified in Step 4. Because of this coupling between Steps 4 and 5, each can impact the other. For example, a calculated high loading (from pressure, temperature, or radiation) in a component may serve to disable it, thereby impacting an accident scenario.

6. Construct and quantify probabilistic load and capacity distributions relating to the figures of merit analyzed to determine the probabilistic safety margin.

7. Determine how to manage uncharacterized risk. Because there is no way to guarantee that all scenarios, hazards, failures, or physics are addressed, the decision-maker should be aware of limitations in the analysis and augment it by adhering to protocols of "good engineering practices."

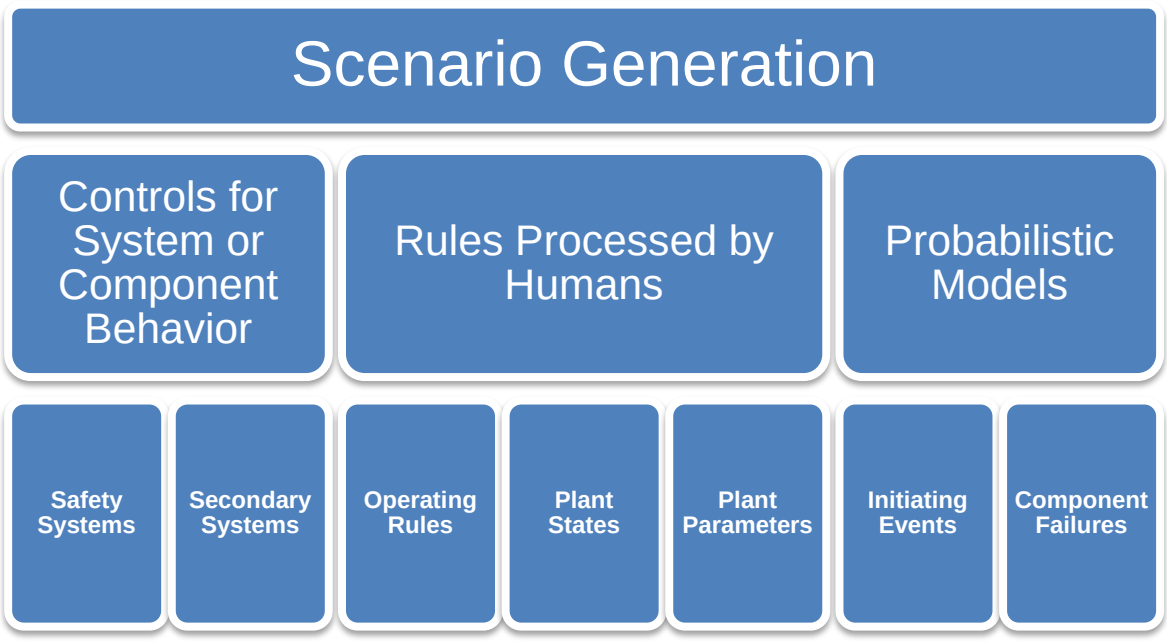

Figure 2. Elements of scenario generation via simulation.

While the simulation-based approach to risk assessment has become better understood, its integration with traditional risk tools and approaches remains an open topic.

2.2 Risk Assessment Tools

The following provides summary descriptions of the PRA codes used to support risk assessment activities at commercial NPPs operating in the U.S. This section also describes derivative codes used to support operational decision-making (particularly with respect to configuration risk management programs) at NPPs. Finally, it provides summary descriptions of advanced tools currently in development and anticipated to be applied over the next several years.

2.2.1 Risk Assessment Tools

2.2.1.1 SAPHIRE

The Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) [10] is a software application developed for performing PRA analyses using PCs that operate via Microsoft Windows. SAPHIRE was developed by Idaho National Laboratory for the U.S. Nuclear Regulatory Commission (NRC). In the U.S., this code is used for individual plant PRA models developed by the NRC (under the Standardized Plant Analysis Risk [SPAR] Model Program). These SPAR models are used for regulatory reviews of plant events and confirmatory evaluations of licensee-proposed RI applications.

SAPHIRE enables users to supply basic event data, create and solve fault and event trees, perform uncertainty analyses, and generate reports. Using the SAPHIRE code, analysts can perform PRAs for any complex system, facility, or process. For NPP PRAs, SAPHIRE can model a plant's response to initiating events (IEs), quantify core damage frequencies, and identify important contributors to core damage (Level 1 PRA). The program can also be used to evaluate containment failure and release models for severe accident conditions given that core damage has occurred (Level 2 PRA). In so doing, the analyst can build a PRA model that assumes the reactor is initially at full-power, low-power, or shutdown conditions. In addition, SAPHIRE can analyze both internal and external events and, in a limited manner, quantify the frequency of release consequences (Level 3 PRA).

Documentation for several recent versions of SAPHIRE was prepared for the NRC and made publicly available on their website. Documentation for SAPHIRE 7 is provided in NUREG/CR 6952 [11], while documentation for SAPHIRE 8 is provided in NUREG/CR 7039 [12]. Each report is published in seven volumes. The manuals for the most recent version of SAPHIRE (Version 8) consist of the following volumes:

- Volume 1 – Overview and Summary
- Volume 2 – Technical Reference
- Volume 3 – User’s Guide
- Volume 4 – Tutorial
- Volume 5 – Workspaces
- Volume 6 – Quality Assurance
- Volume 7 – Data Loading

2.2.1.2 Integrated Risk Technology

The EPRI-developed Risk and Reliability Workstation (or "R&R Workstation") is a comprehensive computational suite for conducting PRA analyses [13]. Within this workstation, the fundamental PRA software program is the Computer Aided Fault Tree Analysis System (CAFTA) [13]. CAFTA is used to create, edit, and quantify reliability models by utilizing fault and event trees. CAFTA can build PRA models to assess the frequency of Level 1 (core damage) occurrences and Level 2 (large early release) events. Given a set of initiating events, basic events, and operator actions, CAFTA will quantify any gate of the fault tree. CAFTA is used to perform the following analyses:

- Develop, manage, and evaluate fault and event trees.
- Generate and analyze cut sets.
- Evaluate the impact of common-cause events.
- Perform Bayesian updating of plant equipment failure data.
- Analyze modeled events and evaluate their outcomes.
- Perform risk-ranking evaluations.
- Conduct sensitivity studies.

CAFTA interfaces with multiple programs in the EPRI R&R Workstation's suite of risk assessment tools in order to permit rapid, comprehensive risk assessments. The R&R Workstation contains the following modules [13]:

- ACUBE (Advanced Cut Set Upper Bound Estimator) – This post-process quantification of cut sets provides a mathematically accurate answer for a specified number of cut sets. It is primarily used for models that have events with large failure probabilities and for which the rare-events approximation is invalid.
- DPC (Direct Probability Calculator) – Performs fault tree quantification without cut sets.
- PRAQuant – Quantifies any gate in a batch mode and can specify different conditions for each quantification run.
- UNCERT – Performs uncertainty propagation.
- FRANX – Supports the integration of analyses (e.g., fire, seismic, flooding, and other external hazard events) into plant PRA models. The R&R Workstation also provides additional modules to support more efficient and effective management and maintenance of plant PRA models.

Since the R&R Workstation was developed by EPRI, it is predominantly used by operating utilities in conducting plant risk assessments. CAFTA was developed—and is currently maintained—under a quality assurance (QA) program in compliance with U.S. 10CFR50 Appendix B and ISO 9001 requirements. All other codes are maintained under EPRI's augmented QA program.

2.2.1.3 ATHEANA

A Technique for Human Event Analysis (ATHEANA) is an approach for developing and evaluating human failure events (HFEs) for HRA at NPPs. ATHEANA provides insights into how operator responses to equipment failures and accident scenarios impact the probability of core damage (Level 1 PRA) and the release of radioactive material into the environment (Level 2 PRA). The ATHEANA methodology is used to accomplish the following objectives:

- Identify scenarios in which operational errors are likely to occur.
- Determine possible error-forcing contexts.
- Determine applicable human-performance-shaping factors.
- Develop HEPs for incorporation into the plant PRA model, including both errors of commission and errors of omission.
- Identify and analyze possible recovery actions.

Results of the ATHEANA technique are incorporated into Level 1 and Level 2 PRAs. These results can also be used to support the determination of appropriate success criteria, the identification of plant vulnerabilities based on weaknesses in normal and emergency operating procedures, and the identification of various personnel interactions that could impact estimated error rates. The ATHEANA methodology is documented in the ATHEANA User's Guide [14], which provides guidance on using ATHEANA to perform HRA. It also describes the qualitative and quantitative analysis approaches encompassed within ATHEANA. The report outlining the technical basis for ATHEANA [15] discusses the overall methodology and provides guidance for employing it.

2.2.1.4 HRA Calculator

The HRA Calculator is a computer program developed by EPRI for performing HRA. It can create and record HFEs and quantify HEPs. The HRA Calculator is used for the following purposes:

- To provide qualitative information on operator responses to accident sequences for inclusion in PRA fault- and event-tree models.
- To provide quantitative estimates of the probability that human error will occur during accident mitigation.
- To evaluate the effects of operator actions.
- To determine whether plant personnel have sufficient time to complete actions identified as important to prevent or mitigate accidents.
- To provide insights into areas where operator training and plant procedural changes could help successfully mitigate accidents.

HRA Calculator results are used to evaluate accident sequence models and determine the extent to which operator actions may contribute to the occurrence and progression of a risk-significant event. The latest version of the HRA Calculator is Version 5.2, released in 2017 [16].

2.2.2 Operational Risk Management Tools

2.2.2.1 Phoenix Risk Monitor

The Phoenix Risk Monitor (PRM) code was developed by EPRI as an all-modes and all-hazards risk integration and visualization tool. Development was initiated in 2009 with the development of a comprehensive functional specification [17]. The most recent release of the software (Phoenix Risk Monitor v2.0) came in November 2017 [18] and is available free-of-charge to EPRI member companies, and to non-members for a nominal charge.

Currently, PRM is primarily used as a tool for plant CRM programs in performing risk management activities related to NPP maintenance during both operating and outage conditions. In this application, PRM replaces the EPRI Equipment Out Of Service code when used to monitor the availability of important SSCs. As with Equipment Out Of Service, PRM provides the following functions to support plant CRM programs:

- Propagate information from the plant PRA model based on plant configuration and evaluate changes to the plant configuration as they occur.
- Quantify risk measures specified in the plant PRA model.
- Translate fault tree results into lists of risk-significant and risk-relative activities, and provide color-coded status panels for use by plant personnel, including operators and plant management.
- Allow users to determine if scheduled work activities require special contingency actions due to estimated increases in risk.

The program allows plant personnel to determine recommended improvements to plant safety based on risk significance. PRM allows users to update work schedules as plant configuration changes occur (i.e., SSCs become unavailable or are returned to service), providing the necessary information for schedule adjustments based on risk assessments. PRM also supports plant-monitoring of online maintenance, as required under Section (a)(4) of the Maintenance Rule. PRM was developed and is maintained under a QA program in compliance with U.S. 10CFR50 Appendix B and ISO 9001 requirements.

2.2.2.2 PARAGON

PARAGON is a multi-purpose software platform tool intended for use by NPP personnel to foster operational “real-time” decision-making. The primary focus of PARAGON is to support comprehensive implementation of CRM programs to comply with Section (a)(4) of the Maintenance Rule (10CFR50.65) across all modes of plant operation. The tool uses a blended approach to support risk assessment and management.

PARAGON provides the following functionality:

- Provide qualitative measures of safety via use of decision trees (for example, assessment of identified key safety functions).
- Provide quantitative estimates of plant risk by:

- interfacing with available PRA quantification software used at operating NPPs (e.g., CAFTA, WinNUPRA, RiskSpectrum)

- assessing impacts from external hazards (earthquakes, flooding, etc.) on plant risk

- conducting probabilistic shutdown safety assessments

- Provide the capabilities to combine quantitative results with deterministic results and other qualitative information to support real-time, RI decision-making.

- Provide user flexibility in specifying plant-specific decision thresholds, affording the ability to assign safety classifications and values based on absolute or relative increases in plant risk.

Setting up a PARAGON model to perform CRM typically includes a combination of qualitative and quantitative features with customized results displayed for PRA personnel, operators, and work planning users. In supporting online maintenance, PARAGON provides a wide range of metrics for use in risk management. These include results for configuration CDF and LERF, cumulative values of these metrics over specified periods of time (e.g., annually), and remain-in-service and return-to-service prioritization lists. PARAGON utilizes graphic profiles for quantitative measures of risk, while qualitative measures of risk are provided via guidance and defense-in-depth evaluations (e.g., safety functions, plant transients, support systems, remain-in-service and return-to-service prioritization). For supporting outage risk assessments and management activities, PARAGON evaluates a variety of critical parameters, including CDF, LERF, and frequency of reactor coolant system boiling. It also provides the capability to estimate decay heat level, time-to-boil curves, and time-to-core damage for loss-of-decay-heat-removal events.

2.2.3 Advanced Tools

2.2.3.1 EMRALD

EMRALD [19] is a dynamic PRA tool being developed at Idaho National Laboratory based on three-phase discrete event simulation. Traditional PRA modeling techniques are effective for many scenarios; however, it is difficult to capture time dependencies and dynamic interactions using the current generation of PRA methods and tools. EMRALD modeling methods are designed around traditional methods yet are structured to enable the analyst to probabilistically model sequential procedures and see, through time, the progression of events that caused the outcome. Compiling the simulation results can reveal probabilities or patterns of time-correlated failures. EMRALD focuses on the following key aspects related to PRA evaluations:

- Simplify the modeling process by providing a structure that corresponds to traditional PRA modeling methods.

- Provide a user interface that makes it easy for users to model and visualize complex interactions.

- Allow users to couple EMRALD with other analysis applications, including physics-based simulations. This includes one-way communication for most applications and two-way loose coupling for customizable applications.

- Provide the sequence and timing of events leading to the specified outcomes.

EMRALD utilizes an open communication protocol using the common messaging platform Extensible Messaging and Presence Protocol [20]. This architecture allows for easy coupling with other engineering tools, permitting direct interaction between the PRA model and physics-based simulations. As a result, simulated events can more directly drive the PRA model, with sampled PRA parameters being fed back into the simulation environment to provide a more accurate evaluation of the impact on plant risk. As a result, these capabilities enable PRA models to match real environment and operation conditions more realistically to human procedures.

2.2.3.2 RAVEN

RAVEN [21, 22] is a software framework able to perform parametric and stochastic analyses based on the response of complex system codes. RAVEN is a multi-purpose stochastic and uncertainty quantification platform capable of communicating with any system code used to perform NPP safety analyses. RAVEN's application programming interfaces allow it to interact with any desired system code, if all the parameters needing perturbed are accessible by input files or via Python [23] interfaces.

RAVEN provides a flexible, multi-purpose framework for uncertainty quantification, regression analysis, PRA, data analysis, and model optimization. Depending on the tasks to be accomplished, as well as on the probabilistic characterization of the problem, RAVEN perturbs (via Monte-Carlo, Latin hypercube, reliability surface search, etc.) the response of the system of interest by altering its own parameters. The system interfaces with third-party software (e.g., RELAP5-3D, MAAP5, etc.), either directly (software coupling) or indirectly (via input/output files). Data generated by the sampling process are analyzed using classical statistical and more advanced data mining approaches. RAVEN also manages the parallel dispatching (both on desktop/workstation and large high-performance computing machines) of the software representing the physical models. RAVEN heavily relies on AI algorithms to construct surrogate models of complex physical systems to perform uncertainty quantification, reliability analysis (limit-state surface), and parametric studies.

3. Proposed Research Roadmap

3.1 Overview

The challenges presented in Section 2 highlight the need for future research activities. Therefore, input was solicited from various members of the PRA community to develop the following proposed research roadmap. The main objectives of the roadmap are:

1. To present the research activities with sufficient detail to understand the issue being addressed and the scope of work.

2. To identify the respective challenges benefitted by each activity (i.e., the value produced by addressing the issue).

3. To estimate the timeline required for completion in relative terms.

4. To prioritize based on perceived benefits to various stakeholders in the nuclear industry.

With these goals in mind, the following sections present the research activities in order of prioritization based on perceived benefit and estimated timeline for completion. For example, an item perceived to be of high worth and relatively short duration will be presented before an item perceived to be of lower worth but also of short duration. If activities are dependent or build upon each other, this will also be noted and accounted for in the timeline estimates. It should be noted that this prioritization represents an initial assessment based on reviews conducted with various industry stakeholder groups. This prioritization is an initial assessment and will likely change over time as conditions (internal and external to the industry) change. As such, the proposed research roadmap should be viewed as a living document that will be updated periodically to reflect changing conditions and stakeholder needs.

3.1 Near-Term Strategic Benefit Activities

3.1.1 Quantification Speed to Support Decision-Making

It is no coincidence that both the first item in Section 2 and the first item prioritized in this section relate to quantification speed. Quantification speed affects all aspects of RI operations and decision-making. When models take a long time to quantify, they delay decisions and create roadblocks to gathering insights. Therefore, the highest perceived benefit to both the PRA community and the nuclear industry comes from research activities that result in decreased quantification times (but still maintain acceptable levels of quantification accuracy).

Options to address quantification speed are vast; however, some may offer relatively high benefits over the short duration necessary to complete the research. For instance, as the industry continues to create multi-hazard models (e.g., internal-events, fire, internal-flood, and seismic models) and prepares to eventually be required to use them in CRM decision-making, it is not feasible to utilize the same truncation value as in the base model. For example, some SPRA models require a truncation of around 1E-12/yr for CDF estimates and can produce cut sets that number in the millions. When such models are combined with models of other hazards that contain similar numbers of cut sets, quantification times can be prohibitively slow. Unlike internal-events models, which have enjoyed decades of refinement, research, and use, FPRA, internal flood PRA, and SPRA models are new to plant operators, who need to evaluate them to support real-time decision-making in such things as plant CRM applications (e.g., scheduling online plant maintenance, addressing an emergent SSC failure, etc.). As a result, it would be

beneficial to conduct research on the appropriate truncation values for these new multi-hazard models, especially in the context of gaining insights from CRM tools used in real-time applications. It is most likely unnecessary to have very low truncation frequencies and generate enormous amounts of cut sets in order to make the correct decision about a particular configuration. By providing justification for the use of higher, more appropriate truncation values, quantification times will automatically decrease.

Another option regarding research to address this issue is to achieve a better understanding of model structures and their impact on quantification times. When discussing this issue with PRA practitioners, many opinions, observations, and anecdotal evidence was offered to suggest how models could be quantified faster. However, concrete guidelines and best practices have not been established for use by practitioners, nor for the multitude of PRA software tools currently in use across the industry, as outlined in Section 2.2. This proposed research topic would include testing various model structures using some of the most common quantification engines available to determine the optimal model structure for various situations. For example, it was observed that wider trees (e.g., less gates in a series) quantify faster with the FTREX engine. Such observations warrant further research and testing to foster an understanding of the generic implications and provide best-practice guidance. The research could also include impacts due to event-tree ordering, usage of certain exclusion gates, and other common modeling techniques shown to slow down quantification speeds.

3.1.2 Dependency Modeling of Human-Related Basic Events

HRA modeling, an accepted practice in modern PRAs, represents baseline human actions as part of a scenario. However, a challenge exists when multiple human actions appear in a single scenario. A key question is how these separate events interact through dependency factors such as events that are close in time or rely on the same staff to accomplish multiple tasks. Current approaches focus on manually determining the degree of dependency through simple rules; however, this identifies only a limited number of combinations, and application of this approach results in complicated models that must be built, analyzed, and understood.

To address the HRA dependency challenge, an automated approach could possibly be developed to identify and apply dependency factors.

3.1.3 Integration of Multi-Hazard Models

Multi-hazard models are increasingly commonplace for both meeting regulatory requirements and supporting plant implementation of various RI applications. The ability to assess the risk generated by all issues—both internal and external—involving the plant is critical to proper implementation of risk-related decision-making. However, these models are relatively new to the industry, with most of the research focused on methods to obtain accurate answers (relative to both the phenomenologies themselves and their resultant impacts on the plant). As a result, little to no research efforts have been made to construct the models for providing efficient calculations. A research project on this topic should include how to structure the underlying tree in which hazard-specific logic gets inserted, but still allow the internal-events model to function properly. There may be an optimal way to manage these structures so as to enable simultaneous work on all the hazards and the internal event logic while still maintaining the connection among all these models. For example, recent industry experience indicates that, when integration is required to create a single top model, the process is more seamless and efficient.

Once the multi-hazard model is created, a parallel research topic with quantification speed (Section 3.2.1) should be explored. These models tend to quantify slowly, delaying any decision-making process involved. This has impacts when used for routine applications such as scheduling maintenance activities, likely precluding effective use of PRA tools to support decision-making during events featuring

significant time constraints (e.g., during external-hazard-induced events at the plant site). Re-structuring the logic could lead to faster quantification times, greatly benefitting all operating reactors. Additionally, all multi-hazard models require exact probability calculations in which the rare-events approximation is not appropriate, meaning that a separate process will further slow down the procurement of a quantified answer. Another useful research topic would be to investigate different calculation methods that allow for faster quantification and produce more accurate answers, either by intelligently splitting up the model so that exact answers are calculated for those hazards that require them, or post-processing in a way that targets only the cut sets that would most benefit from performing an exact calculation.

Lastly, integrated multi-hazard models have difficulty presenting risk metrics across all the hazards. For example, internal-events models typically use the MCUB estimation and report the Fussell-Vesely importance measure as a percent contribution to the overall answer. This contrasts with seismic PRAs, in which the answer is estimated by calculating the exact frequency for a subset of cut sets along with the MCUB estimation on the remaining cut sets. This approach makes calculating Fussell-Vesely impossible, and criticality is instead used to approximate the percent contribution to the overall answer. In multi-hazard models, the cut sets are inseparable, and these calculation methods are not compatible across all hazards.

3.1.4 Improve FLEX Data for Equipment and Operator Reliability

Commercial NPP safety capabilities continue to expand as our understanding of new hazards grows. Following the accident at Fukushima Daiichi, the flexible operations (FLEX) program [24] was initiated at all operating NPPs in the U.S. (which have capabilities like most international NPPs). The initial concept behind FLEX was to provide a temporary means of restoring key safety functions during an extended-loss-of-AC-power or loss-of-ultimate-heat-sink (LUHS) event, or both. As the implementation scope was discussed with the regulator, the scope and pedigree of the equipment grew to the point that FLEX is now a major program at every operating NPP in the U.S. Its capabilities are redundant, the equipment is monitored, and all operators are trained on the implementation procedures. Thus, FLEX represents a major enhancement in the safe operation of NPPs; however, PRA models have been slow to incorporate useful capabilities to evaluate and quantify these improvements.

This is largely due to two reasons. The first is the lack of data associated with the FLEX equipment procured and stored either onsite or at one of the two regional centers. The second is the lack of data and accepted methods to evaluate operator reliability in implementing the strategies. While equipment reliability has long been a staple in updating failure probabilities of SSCs in PRA models, FLEX equipment is relatively new compared to the safety-related equipment permanently installed in operating plants. Additionally, testing has been carried out on the equipment (for various reasons) over the years and added to the collective pool of data available to analysts. FLEX equipment needs the same treatment. An effort to collect data from utilities where testing has occurred should be considered top-priority—the optimal strategy. The pooled data can be analyzed to provide the PRA models with a useful estimate of failure probabilities for FLEX equipment, and to document the justification behind those values. However, because full-scale testing may not be feasible or cost-effective, or the data pool may be too limited, alternatives for generating the data should be considered, researched, and implemented for use in industry PRA models. As models become more complex and NPP capabilities grow, refusing to allow certain strategies or additional equipment into the models because of lack of data seems inappropriate given the investment in FLEX already made by nuclear operators.

3.1.5 Acceptance Criteria for Model Details in Various Risk-Informed Applications

Use of risk-informed (RI) applications continues to expand throughout the U.S. NPP fleet. The strength of RI applications lies in leveraging already-existing comprehensive PRA models to gain

valuable insights into the relative risk of performing various activities while at power. Expansion of the RI program led to increased development of models to cover both the internal and external hazards at the site. However, increased model complexity poses new challenges when utilizing multi-hazard models to support decision-making activities. The primary challenges are quantification speed and computer memory limitations. These are largely set by quantifying individual hazard models to determine the appropriate model detail level and truncation value to achieve convergence in accordance with the criteria specified in the ASME/ANS PRA Standard [25]. This level of model detail and cut-set production may not be warranted for an RI application that reviews multiple hazard models for risk insights into the planned activity. Therefore, it is proposed that a research activity be performed to review these models and develop guidance and acceptance criteria with respect to model detail and truncation limits for individual (or all) RI applications. This activity is important for setting a baseline expectation that supports valuable risk insights for each RI application, as well as sufficient quantification speed for real-time decision-making.

3.1.6 Model Modification Simplification and Documentation Assistant

In current legacy tools, when equipment fails or other abnormal conditions occur that need to be modeled in the PRA, a manual process for creating text files containing commands to alter the model prior to quantification must occur. This involves locating the basic events or gates that require alteration, listing the model element to be changed, attaching the file to the quantification output, and re-running the model. However, multiple cases or various sensitivities may need to be run for each model update or application. This can cause many files to be produced—with many new cut-set files for each case—and documentation of all the results can be cumbersome to maintain, as well as prone to error.

This proposed research topic would include developing a graphical user interface (GUI) to interact with the model, thus assisting PRA practitioners in developing new model configurations for various types of RI applications. For example, the GUI could leverage already-existing SSCs to BE mappings now common to fire or seismic PRAs. The user could disable the SSC, setting all BEs mapped to the SSC to TRUE for the run, or have another setting that allows the user to set an HFE to FALSE (simulating perfect performance) for a sensitivity run. The GUI should be accessed when quantifications are to be performed, and it should allow for case names to be applied, saved, and utilized by all output files. A co-developed documentation assistant application could furnish a report describing the modeling changes and all names, files, and notes attached to that particular run. Some of these capabilities exist in EPRI's PRAQuant tool; however, there is currently no way to access a GUI for information on model changes or to automatically generate a report to assist the user in creating the documentation.

3.1.7 Expanded Usage of Risk-Informed Applications

Success in developing the current RI applications used in operating the U.S. NPP fleet led to industry's desire to expand the approach into new areas. There are several potential candidates for an RI framework to be created; however, research is needed to determine the appropriate modeling techniques, insights, and application for each initiative.

The most requested RI framework is for security. Security requirements at most U.S. NPPs have grown in scope and size of the work force. Such requirements were largely developed after the terrorist attacks on September 11th, 2001, and additional protocols have been added ever since. Risk information was never developed for these modifications or procedures, and models do not currently exist for gaining insights into the most effective response tactics. A potential research project could include investigating the criteria that would be required to best risk-inform the security programs at U.S. NPPs, including utilizing existing model information to understand risk-significant components and develop new models that review entry points, SSC vulnerabilities to different methods of sabotage, and the security team's

response to such scenarios. Metrics for recognizing a change to the current design must also be considered to provide confidence that the change will not be detrimental to the plant security program. It should be noted that developing an RI approach to nuclear plant security is complicated, since much of the information necessary for performing risk assessments is considered safeguard-related and cannot be made available to risk analysts. Access to the review and approval processes (for both the plant owner/operator and the regulator) are also limited. Therefore, though the potential exists to generate large savings via an RI approach to plant security, successfully developing such an approach and obtaining those savings could be a challenge.

3.1.8 Improving Models Used for Time-Dependent Approximations

Time is becoming increasingly important to risk analysis models. Time enters the risk calculation in several possible ways, including:

- Competing processes such as recovery of offsite power, diesel generator recovery, and duration of station batteries when modeling station blackout scenarios.
- Human activities such as FLEX operations, when multiple steps must be considered to determine the successful operation of backup power or cooling water.
- Longer mission times (beyond 24 hours) may require deeper consideration of time-related interactions, including operational questions such as the recovery of failed components.
- Some hazards (e.g., flooding and fire) raise the question of delays, and the rate at which the hazard changes over time (e.g., flood rise rate, fire spread rate) determines the hazard's overall impact on the plant.

Being able to directly represent these types of timing considerations will improve the realism of the risk models, but the complexity of any modifications must first be considered.

3.1.9 Sequence Success Term Recovery

External-hazard models pose a challenge to the PRA community by containing events that can occur relatively frequently (and for which the rare-event approximation is not appropriate) and have induced failure probabilities that may contribute significantly to the overall contribution of the end state being quantified. Calculating an exact probability for the logic structure in modern PRA models leads to resource issues, particularly regarding computer memory, as the equations quickly become too large to handle. A possible research opportunity is to determine the most appropriate way of calculating more exact probabilities within the current risk-modeling framework. This could include reviewing how sequences handle success terms and how they might apply a recovery to the non-rare events contained in the model. Benefit would come from eliminating the need to post-process the results using a separate binary-decision-diagram algorithm to generate a more accurate answer. While a more accurate answer is desirable, meaningful risk metrics for individual events are also important for utilizing the model to its fullest potential. Therefore, a method to develop compatible risk metrics using rare-events models would be valuable in effective decision-making. This activity overlaps with those described in Sections 3.2.1 and 3.2.2.

3.1.10 Application Interfaces Between PRA Tools

Building PRA models requires information from a variety of sources. Analysis of how the plant operates, the system design, and the plant's response to accidents and external events are just a sampling

of the types of information that should be included in a model. With so many ways to perform analyses, collect data, and transform them into a format that can be incorporated into models, interfaces with various tools becomes a necessity. It is not uncommon for PRA practitioners to leverage spreadsheet and database tools (such as Microsoft Access or Excel) to manipulate data and perform calculations, only to have to manually insert the new information into a PRA software tool.

A potential area for research could include better application programming interfaces between commonly used tools such as Access or Excel and PRA-specific software like CAFTA or SAPHIRE. A standard data format or set of functions to automatically detect, translate, and insert data into PRA-specific software for use in the models would greatly decrease the effort in developing new tools, while increasing collaboration among various users, such that tools developed outside one PRA-specific ecosystem could be used by someone in another ecosystem. A review of the available technologies, commonly used tools, and their functions and data structures is vital to developing the most universal product possible.

3.2 Longer-Term Activities

3.2.1 Automate Dynamic Failure Models from Existing PRAs

The ability to use more advanced methods that include time or physics is becoming more widely available. However, there needs to be a way to automatically generate and use dynamic models from existing PRA models (e.g., fault and event trees) to allow for easy dynamic analysis. For example, templates that represent specific dynamic systems and can be reused in existing models, or applying adjustment factors to models, may be applicable. Included in this application would be ways to integrate the different types of models into one framework, such as being able to query scenarios to see whether the thermal hydraulics indicate any core damage.

3.2.2 Improvements to Support System Fault-Tree Modeling

IE frequencies for nuclear industry PRAs and the NRC SPAR models are generally based on data collection efforts to quantify these frequencies. For rare but potentially high-consequence initiators representing the failure of support systems, this approach has a few shortcomings:

- There are no complete system failure events in the available datasets.

- The frequencies of these initiators might reasonably be expected to vary from plant to plant, due to design variations and environmental factors. The data collection effort cannot estimate the resulting plant-to-plant variability in IE frequency using such sparse event-count data.

- The importance, with respect to core damage, for components in these systems is underestimated when the PRA models represent only the event-mitigation aspect of components in these systems, without including the IE contribution.

Another argument in favor of calculating such IE frequencies from suitable models is that, while system failure events might be too rare to appear in the datasets, component failure events in the support systems are more frequent. Thus, the component failure rates are relatively well-known. Therefore, what is needed is a suitable method for calculating the IE frequency (expected number of system failures over some operating mission) from known component failure rates while incorporating issues such as dependent failures. However, current modeling practices result in complicated models, as illustrated in Figure 3. Approaches to simplify this type of model would help ensure a better understanding of PRAs that use this approach to represent support systems.

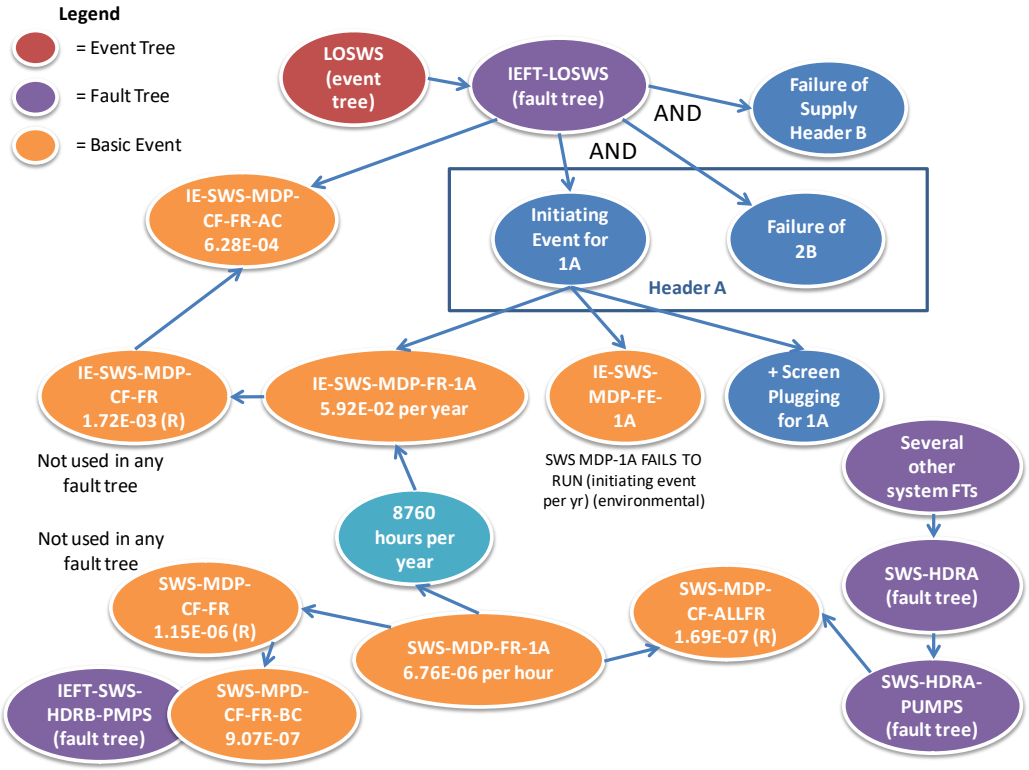

Figure 3. Example basic event relationships for a support system fault-tree model.

3.2.3 Uncertainty Analysis

The relative lack of failure rate data at NPPs can be problematic when performing meaningful uncertainty analysis. The effort described in Section 3.2.3 recommends gathering data on FLEX equipment reliability and operator performance to support placing this equipment in service when needed. A possible research activity could include gathering more reliability data on critical SSCs at NPPs during the effort to collect data on FLEX equipment. That way, the collection effort only needs to be performed once, and a large amount of data would become available for industry to use. Another potential research topic is how to best apply the additional data to perform meaningful uncertainty calculations—with a emphasis on how the uncertainty information could best be used in decision-making processes. Incorporating the data into a software tool that can provide risk insights within a reasonable timeframe would be warranted to upgrade the uncertainty-related capabilities of existing risk models.

Research could also include developing a software tool that accepts uncertainty parameters without equations. Recently, seismic- and high-wind-hazard analysts claimed it impossible to represent the uncertainty bands via a simple equation or distribution. Therefore, another method of applying uncertainty parameters should be considered for these hazards and their unique characteristics, as well as respective estimates of the phenomena hazard curves. Then a research effort could focus on how to combine multiple models' uncertainty distributions in a way that gives unique insights.

3.2.4 Integration of Multi-Unit Models

One outcome of the Fukushima Daiichi accident was the understanding that an event/accident at one unit of a multi-unit site could have significant consequences for all the co-located units. Currently, assessment of plant risk via PRA assumes the (nearly) complete independence of the different units (except in the case of plant support systems that service all units located at the site). This includes an assumption that the occurrence of an accident at one unit does not impact the estimated conditional risk of the other units, as estimated by the PRA models. Since the Fukushima Daiichi accident, this assumption has come under increased scrutiny and question, leading to efforts to evaluate how to address this limitation. In particular, this event demonstrated that a multi-unit reactor accident could occur and a combination of external hazards could negate the plant's designed defenses. This recognition led to efforts within the international community to develop approaches to address the likelihood and potential impact of events at sites containing more than one operating nuclear unit. Initial work was conducted to review precursor events that could potentially simultaneously impact multiple units at an NPP site. [26] These were primarily externally induced events (such as the flooding event at the Le Blayais plant in France in 1999 and the seismic event at the Kashiwazaki-Kariwa plant in Japan in 2007). This initial work also evaluated previous industry efforts to perform multi-unit PRA evaluations, particularly in regard to the Seabrook Station Level 3 PRA. This IAEA report recommends that considerations be made to address PRAs for multi-unit NPP sites. It is noted that this work is still at an early stage and significant additional research is needed to develop, demonstrate, and mature the approaches. Such an effort is relevant due to the fact that, from the perspective of regulatory policy, the degree to which an accident at a nuclear plant site ultimately impacts the public depends on the level of fuel damage and subsequent release of radioactive materials to the total inventory of fuel contained onsite (at all the reactors and in all the various states of use and storage).

3.2.5 Linking Raw Data to Basic Events for Automated Failure Rate Updates

During the model update process, gathering and processing raw performance data is part of the required activities. This raw data is utilized to update the failure rates associated with components and ultimately modify the probability of failure for the modeled SSCs in a way that conforms with plant and industry operational experience. This process can be time-consuming, cumbersome, repetitive, and prone to human error. A potential research area could include reviewing the format of plant-supplied data and developing a methodology and/or tool for importing the raw data into a database, processing the data, and linking the PRA model database to the failure-rate database for automated incorporation into the plant PRA model. If the data supplied from the sites appears divergent, a standard could be researched and proposed, and a tool created to provide a common framework for evaluating, analyzing, and incorporating the data updates. The benefits would be decreased effort and improved efficiency during the model update process and development of estimates and results less prone to human error.

3.2.6 Streamline Model Maintenance Process with Declarative Modeling

As with other activities related to PRA modeling, the update process is largely a manual (and therefore expensive) effort. The update process, required by the ASME/ANS PRA Standard [25], requires periodic updating of data, as discussed in Section 3.3.5, but also reviewing of plant changes, piping and instrumentation diagrams, and other 3D models from plant information systems in order to manually update the fault trees to reflect plant as-built/as-operated conditions. Generally, details are added to a fault tree only when an application draws attention to a simplification or assumption made about that system, yielding an unacceptably conservative result. Therefore, aspects of the model's accuracy are dependent on human review and circumstance. A potential research activity could involve investigating ways to automate the model-creation process, with additional details provided via declarative modeling.

Declarative modeling would assist the PRA community by developing an algorithm to review plant design materials to extract data and create logic structures that represent the plant systems as documented. This could lead to increased overall detail for systems that might not otherwise have such details included. It may also reduce errors in reviewing/building logic structures through interpretation. Although a level of review will always be needed to ensure the algorithm creates the appropriate relationships, the reduced effort from building more detailed models would far outweigh the effort to review the modeling outputs. This would have overlapping benefits to Section 3.3.5 in regard to linking raw data to BEs in the model for automated data updates.

3.2.7 Artificial Intelligence in Risk Management

As the field of AI grows and the capabilities of different systems expand, use of AI in PRA model development, analysis, and maintenance could greatly benefit the industry. Currently, the creation of a PRA model is a manual process, as described in several previous sections; as such, it is ripe for approaches to automate the creation and maintenance of models. Section 3.3.7 discusses utilizing declarative modeling to enable an algorithm to interpret design drawings, then develop logic structures to represent how they function. One possible avenue for AI assistance in PRA development would be to train the AI algorithm to interpret the piping and instrumentation drawings, procedures, technical specifications, and other design/licensing documents in order to develop the declarative model or logic structures directly from the design elements. This removes the need for human interpretation of the design to develop the logic structure. Of course, human expertise is necessary to develop the programming and to support the training and validation of the algorithms, but this approach has the potential to reduce the time when updating, maintaining, or building models.

Another possible research activity for investigating the use of AI in PRA model analysis would be to scan the fault tree for modeling inconsistencies or inefficiencies. This would tie-in with the sections on quantification speed and allow models to run faster after being reconfigured by the algorithm. Additionally, a separate research activity may include training an AI algorithm to recognize combinations of events across many cut sets or event cut-set files. This could streamline the analysis of HEP combinations or other elements that are multiple events represented in the model by a single event. This effort links to analyzing the models regarding the criticality of combinations of events. It is made difficult using current tools, due to the volume and possible permutations of different events across the cut sets. It is resource- and time-intensive, whereas training an AI algorithm to scan the cut sets for the most important combinations of events then either report back those combinations for further analysis or interface directly with the PRA software to test for criticality would be a huge advancement in the analysis of PRA models, particularly in regard to FPRA models.

4. REFERENCES

1. "Insights on Risk Margins at Nuclear Power Plants: A Technical Evaluation of Margins in Relation to Quantitative Health Objectives and Subsidiary Risk Goals in the United States," EPRI 3002012967, May 2018, Electric Power Research Institute, Palo Alto, CA.
2. United States Nuclear Regulatory Commission (NRC), Inspection Manual Chapters 0609, "Significance Determination Process," Washington, D.C. (2015).
3. National Fire Protection Association, "Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants," NFPA 805 (2015).
4. Nuclear Energy Institute (NEI), "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants, Revision 4b," NEI Report NEI 93-01, Washington, D.C. (2015).
5. Nuclear Energy Institute (NEI), "Risk-Informed Technical Specifications Initiative 5b, Risk-Informed Method for Control of Surveillance Frequencies," NEI Report 04-10, Revision 1, Washington, D.C. (2007).
6. Nuclear Energy Institute (NEI), "10 CFR 50.69 SSC Categorization Guideline," NEI Report 00-04, Revision 0, Washington, D.C. (2005).
7. Nuclear Energy Institute (NEI), "Risk-Informed Technical Specifications Initiative 4b, Risk-Managed Technical Specifications (RMTS) Guidelines – Industry Guidance Document" NEI Report 06-09, Revision 0, Washington, D.C. (2006).
8. "Technical Approach to Probabilistic Safety Assessment for Multiple Reactor Units," International Atomic Energy Agency Safety Reports Series No. 96, May 2019, International Atomic Energy Agency, Vienna, Austria.
9. https://www.iaea.org/projects/crp/i31031 (accessed 4 May 2020).
10. saphire.inl.gov (Accessed 29 April 2020).
11. NUREG/CR-6952, "Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 7."
12. NUREG/CR-7079, "Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 8."
13. Risk and Reliability Workstation, EPRI 1020712, July 2012, Electric Power Research Institute
14. NUREG 1880, "ATHEANA User's Guide," U.S. Nuclear Regulatory Commission, Washington, D.C. (2007).
15. NUREG 1624, "Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)," U.S. Nuclear Regulatory Commission, Washington, D.C., 2000 NUREG-1624, Rev 1.
16. *HRA Calculator Version 5.2*: EPRI, Palo Alto, CA: 2017, 3002010680.
17. *Phoenix Functional Requirements and Roadmap*. EPRI, Palo Alto, CA: 2009, 1019207.
18. *Phoenix Risk Monitor (RM) Version 2.0a – Software*. EPRI, Palo Alto, CA: 2017, 3002011626.
19. https://emrald.inl.gov/SitePages/Overview.aspx (accessed 4 May 2020).
20. https://xmpp.org (accessed 4 May 2020).
21. https://raven.inl.gov/SitePages/Overview.aspx (accessed 4 May 2020).
22. D. Mandelli et al., "BWR Station Blackout: A RISMC Analysis Using RAVEN and RELAP5-3D," *Nuclear Technology*, vol. 193, 161-174, January 2016.
23. https://www.python.org/ (accessed 4 May 2020).
24. NEI 12-06 (Rev 4), "Diverse and Flexible Coping Strategies (FLEX) Implementation Guide," December 2016, Nuclear Energy Institute, Washington, D.C.
25. ASME/ANS, 2013, RA-Sb Standard for Level 1/Large Early Release Frequency PRA for NPP Applications, American Society of Mechanical Engineers / American Nuclear Society.
26. "Technical Approach to Probabilistic Safety Assessment for Multiple Reactor Sites," Safety reports Series No. 96, 2019, International Atomic Energy Agency, Vienna.