http://dx.doi.org/10.5516/NET.03.2014.700

PRA: A PERSPECTIVE ON STRENGTHS, CURRENT LIMITATIONS, AND POSSIBLE IMPROVEMENTS

ALI MOSLEH
Center for Risk and Reliability
University of Maryland, College Park, MD 20742
E-mail : Mosleh@umd.edu

Received February 20, 2014

Probabilistic risk assessment (PRA) has been used in various technological fields to assist regulatory agencies, managerial decision makers, and systems designers in assessing and mitigating the risks inherent in these complex arrangements. Has PRA delivered on its promise? How do we gage PRA performance? Are our expectations about value of PRA realistic? Are there disparities between what we get and what we think we are getting form PRA and its various derivatives? Do current PRAs reflect the knowledge gained from actual events? How do we address potential gaps? These are some of the questions that have been raised over the years since the inception of the field more than forty years ago. This paper offers a brief assessment of PRA as a technical discipline in theory and practice, its key strengths and weaknesses, and suggestions on ways to address real and perceived shortcomings.

KEYWORDS : Probabilistic Risk Assessment, PRA Applications and Lesson Leaned, Advanced PRA Methods

1. INTRODUCTION

Probabilistic risk assessment (PRA) is now a well-established discipline with growing applications in support of rational decision-making involving important technological and societal risks. Risk analysis provides a common platform for technical exchanges on safety matters between key stakeholders, such as regulators, industry managers, and system designers and operators. By doing a PRA we seek to

- Determine potential undesirable consequences associated with use of systems and processes
- Identify ways that such consequences could materialize
- Estimate the likelihood (e.g., probability) of such events
- Provide input to decision makers on optimal strategies to reduce the levels of risk

In many important applications, however, risk analysis requires a significant investment of resources to be accomplished effectively. In the ideal case, this investment will result in the potential to reduce costs by removing safeguards, redundant equipment, reducing maintenance or inspection requirements, or streamlining operational procedures. Conversely, it provides insight into the scenarios that transpire during a risk event, allowing for identification of areas were additional response capacity is required in order to improve the risk response or other mitigating actions.

After more than 4 decades of methodological developments and many real application applications a fair question is whether PRA delivered on its promise. How do we gage PRA performance? Are our expectations about value of PRA realistic? Are there disparities between what we get from PRA and what we had expected? Do current PRAs reflect the knowledge gained from actual events? How do we address potential gaps? These are some of the questions that have been raised over the years since the inception of the field more than forty years ago.

This paper offers a brief assessment of PRA as a technical discipline in theory and practice, explores its key strengths and weaknesses, and offers suggestions on ways to address real and perceived shortcomings.

2. PRA DEVELOPMENT AND APPLICATIONS

2.1 A Brief History

The genesis of modern PRA methodology was the Reactor Safety Study (RSS), also known as WASH-1400 [1]. The main objective of the study was to produce a "generic estimate" of the risks associated with commercial nuclear power in the U.S. WASH-1400 was the first comprehensive, large-scale probabilistic risk assessment of a complex system. It established the core techniques widely used for PRA of engineered systems. Following the publication of RSS, and during the period 1980-1988, numerous full scope PRAs of commercial nuclear power

plants were performed by the nuclear industry. Major milestones in applications and methodological advancements in PRA included the nuclear industry sponsored Zion and Indian Point-2 and -3 plant–specific PRAs completed in1981 [2.3] where among other findings showed that external events (earthquakes and fires) could be significant contributors to risk of plants, and that the containment failure did not always follow a severe core damage event.

Another important milestone was the completion of NRC-sponsored NUREG-1150 study in 1989. The study took a closer look at severe accidents and containment performance. This was followed by the Individual Plant Examinations (IPEs) conducted by the utility companies in response to the US Nuclear Regulatory Commission (NRC) generic letter [GL 88-20] in 1988 requesting that each licensee in the United States use PRA-like methodologies to perform a plant-specific search for vulnerabilities that might lead to severe accidents. These studies were conducted in the period 1990-2000.

The 90's also witnessed growing interest in the PRA technology internationally, and the efforts by the International Atomic Energy Agency (IAEA) to promote and support of the use of PRA by Member States. In 1995 the US NRC issued the PRA policy statement that directed the NRC staff to use PRA in all regulatory matters to the extent supported by the state of the art, while keeping the defense-in-depth philosophy as the cornerstone of reactor safety and NRC regulatory and oversight function. NRC Regulatory Guide 1.174, issued in 1998, took an important step forward articulating how to use PRA in decisions regarding licensee requests for change in the licensing basis.

2.2 Evolution of PRA Methodology

The framework introduced by WASH-1400 was a simple but powerful mix of deductive and inductive logic model (event tree models with supporting fault trees) and included a defined a level of decomposition (e.g., system failure models based on *functional failure modes* of major components (such as valves, pumps, and batteries), a set of statistical approaches to estimate model parameters (e.g., failure rates) using "generic data" and expert opinion, and an approach to model integration (combining FT and ET logic models) to obtain total risk and intermediate metrics (e.g., core melt frequency) and contributing factors.

The study however left important methodological gaps in a number of areas including

- Formalized inference framework
- Explicit treatment of various dependencies
- Dynamics (including aging effects)
- External events
- Explicit modeling of phenomenological events
- Human and organizational factors
- Software behavior modeling
- Explicit treatment of different types and sources of uncertainty

Over the past 40 years since the publication of WASH-1400, methodological advancements driven by research and applications sponsored by government agencies and industry, have addressed a number of these gaps. Progress has been made by:

- Broader coverage of risk contributors
  - External Events (Fire, Seismic, Energetic Objects, etc.)
  - Human Reliability Analysis
  - Organizational Factors/Management /Safety Culture
- Better treatment of some dependencies
  - Component-Level CCFs
  - State of Knowledge Dependencies
  - Multi-unit Dependencies
- Improved inference methods
  - Bayesian Inference
  - Uncertain Evidence
  - Expert Opinion
- Improved uncertainty characterization and analysis methods
  - Model and Parameter
  - Aleatory and Epistemic
  - Advanced Sampling Schemes
- More advanced computational algorithms
  - Binary Decision Diagram
- Benchmark exercises, peer reviews, standards
- Development of databases and operating experience reporting systems

All these improvements were formulated essentially within the modeling framework of WASH-1400 (which we will call Classical PRA Approach). As such, the advancements have been largely constrained by the framework itself.

2.3 Areas of Application

Risk assessments are normally performed to implicitly or explicitly support decisions under uncertainty. Some applications include:

- Use of quantitative risk measures produced by PRA, in conjunction with other safety measures (e. g., defense-in depth) to meet safety goals
- Use of insights provided by qualitative and quantitative models to steer design and operational aspects of the technological system towards higher levels of safety, in a rational and cost-effective manner
- Application of risk information to o improve operational availability and efficiency

More targeted applications, particularly in the nuclear power industry include

- Significance Determination Programs and Event Assessments
- Precursor studies
- Improving inspection and safety oversight effectiveness
- Performing design trades (for new reactor designs and backfits)

3. PRA PERFORMANCE IN PRACTICE

A question often asked is whether PRAs produce credible numerical values of risk. In search for an answer to this question, first we recognize that most cases where the numerical credibility is of concern involve risk of rare events in highly reliable systems. I such cases risk estimates are unlikely to be verifiable with statistical evidence. However, experience in two important domains of application, namely nuclear power and space missions, provide indications that risk values produced by high quality PRAs can in fact be quite credible.

In the case of nuclear power risk we have the generic estimates of core melt frequencies produced by WASH-1400 in the rage $5x10^{-5}$ to $5x10^{-4}$. This can be compared with the actual global experience of 5 core meltdown events (TMI, Chernobyl, and 3 units at Fukushima) over roughly 10,000 reactor years of operation, that is a core melt frequency of $5x10^{-4}$. In fact this number is also consistent with measures of "central tendency" of the plant-to-plant variability distribution of the core melt frequencies produces by plant-specific PRAs. In addition, systems studies suggest that by applying advanced methods for fault tree modeling, Bayesian probability estimation methods, and properly accounting for dependencies and uncertainties, PRA logic models produce numerical estimates for system failure probabilities that are consistent with the historical evidence, i.e., observed system failure probabilities.

The same is true in another important field of application, the assessment of risks associated with Space Shuttle flights. Several Space Shuttle PRA studies (see for example [4]) sponsored by NASA over the last two decades of space shuttle program produced estimates that were later shown to be very realistic. One estimate calculated the probability of Loss of Crew and Vehicle (LOCV) to be 1/90 per mission. A later full scope Space Shuttle PRA put the number at 1/112 per mission. The actual record was 2/134 accounting for the Challenger and Columbia accidents over the 134 Space Shuttle flights.

Of course both the nuclear power and NASA studies where done essentially with WASH-1400 style (classic PRA) methodologies, which are far more advanced and rigorous compared to earlier attempts in both industries with inferior and largely ad hoc methods. For instance earlier studies prior to WASH-1400 had estimated core melt frequencies several orders of magnitude lower than WASH-1400 values. Similarly for the Space Shuttle program estimates on the order or 1/100,000 per mission were produced. The number was calculated by starting with 1/100 as reference value (historical failure probability for typical space launch vehicles), and then reducing it by factors of 10 as credit for "more advanced technology", "astronauts high levels of skill and training" and similar factors. Such low values of course turned out to be totally inconsistent with the observed risk level.

Another frequent question is whether PRAs produce new qualitative insights. PRAs have successfully identified many vulnerabilities that were unknown, not adequately safeguarded against in the original designs, or simply viewed to be unimportant. For example WASH-1400 highlighted the importance of some beyond design basis risk scenarios and scenarios of the same class as the TMI accident before it happened in 1979. Even though the exact sequence of events that led to the small LOCA at TMI was not in the WASH-1400, but small LOCAs were analyzed in the study.

As another example, PRAs identified and quantified plant vulnerabilities to common cause failure events (CCF). Also through the ranking of risk contributors by probability and consequence, PRAs have provided a consistent basis for prioritization and implementation of many safety improvements and design decisions. Benefits of PRA in the nuclear industry included discovery of relatively significant safety improvements that were possible through the Individual Plant Examination initiative in the late 1980s, risk insights that led to the station blackout rule, which served to reduce the relatively high risk and significance of loss of off-site power events, and improvements in managing shutdown risk and in applying the maintenance rule.

Many insights are of course gained simply by the exercise of performing the PRA, building the model, and understanding the complexities of the system and its accident scenarios, i.e., thinking about "what can go wrong".

When accidents occur involving system for which PRA analysis has been conducted, a frequent question is whether the actual accident scenario was included in the risk analysis. Of course this a legitimate questions, but satisfactory answer is only possible with a common understanding of the PRA modeling paradigm, the scope of the specific PRA in question, and the context and type of decision the PRA was originally designed to support. A common misconception by non-specialist is that PRAs are supposed to include the same, somewhat arbitrary, level of specificity and detail that we choose to view and describe actual risk events. This of course ignores the fact that PRA modeling is done fundamentally by abstracting and clustering of events into classes and categories.

The level of abstraction is a function of the decision being supported by the PRA, state of knowledge (such as level of understanding of the system and its human and physical environment), and availability of resources and suitable methods and tools. Without clustering and binning events into classes of events, assignment of probabilities would not be possible. Extremely detailed delineation of event sequences in the limit essentially means zero probability of occurrence. To address this, PRA is conducted using cluster and classes of scenarios. As these scenarios are amassed, the summation of their individual probabilities highlights the realistic vulnerabilities of the system under evaluation. However, the proper identification of the scenarios to be grouped can provide a challenge to the risk

assessment process. The identification must be complete enough to address the vulnerabilities, but not so specific that it creates grouping categories that are too narrow, which results in discounting the likelihood of the accident occurrence.

So a more meaningful question is whether the observed risk event belongs in at least one of the event classes included in the PRA. This of course leads to the issue of PRA completeness, the ability of PRA to include, within a defined scope, all possible initiators and accident classes before applying screening on the basis of low likelihood or insignificant consequence.

Completeness is a major issue in the theory and applications of PRA. Attempts have been made to quantify the degree of uncertainty in the estimated risk values due to PRA model structure (model uncertainty) and model parameters (parameter uncertainty)[5]. However even if one manages to develop the most credible and accurate quantitative assessment of model and parameter uncertainties, the fact that "unknown-unknowns" by definition would not be included in the risk scenario models (qualitative completeness) is an issue. This is important from a risk management point of view since obviously one cannot develop and implement countermeasures against unknowns.

Needless to say that completeness is not just the breadth of coverage by the risk scenarios, but also their depth of causality, for instance the fidelity of definition of basic events in fault tree and event tree models in conventional PRAs.

4. PRA LESSONS LEARNED FROM ACCIDENTS

One way of assessing the effectiveness of PRA methodologies and also identifying where and how to improve the methods is through analyzing actual events and drawing lessons that can be learned form them. In this section we take a look at three accidents in two domains two where classical PRA methods have been used. The first accident to be discussed is a near-miss, fire-initiated, cascading scenario at the H. B. Robinson Nuclear Power Plant located in South Carolina. The second case is core meltdowns experienced at Fukushima Dai-ichi, NPP site which were the result of a strong earthquake and ensuing tsunami off the coast of Japan. The final case is the Space Shuttle Columbia accident in 2003 initiated by damage caused by impact of debris at launch, resulting in the spacecraft disintegration during re-entry at the end of the mission.

4.1 H.B. Robinson NPP Fire Event

On March 28, 2010, a feeder cable failure to a 4kV non-vital bus at Robinson NPP caused an arc flash and fire. A subsequent failure of a bus-tie breaker to open and isolate the fault resulted in a loss of power to Reactor Coolant Pump (RCP) B and a subsequent reactor trip. Subsequent to the reactor trip, an automatic safety injection (SI) actuation occurred due to an uncontrolled reactor coolant system (RCS) cool-down. Plant response was complicated by equipment malfunctions and failure of the operating crew to diagnose plant conditions and properly control the plant. During plant restoration a relay was reset which re-initiated the electrical fault and caused a second fire.

The event involved a number of equipment failures including

- A feeder cable failure leads to an arc fault and initial fire causing the failure of the Unit Auxiliary Transformer and non-vital Bus 5.
- Breaker 24 failed to open causing the loss of non-vital Bus 4.
- Alternate charging valve CVC-310A opened due the Phase-A containment isolation and air leaks within the valve. This caused seal injection flow to be diverted away from the RCP seals.
- The charging suction source failed to automatically switch over from the VCT to the RWST due to instrumentation failure.

Operator action deficiencies also contributed to the complexity of the event:

- Failed to control the RCS cool-down caused by the opening of the MSR drain valves.
- Failed (initially) to recognize the closure of component cooling water (CCW) flow return valve from the RCPs.
- Failed to recognize the RCP seal injection had become inadequate.
- Failed (initially) to diagnose the failed charging suction switch-over resulting in a loss of charging flow.
- NLO error caused the loss of Instrument Bus 3.
- After the plant was stabilized, operators reinitiated the electrical fault causing a second fire because they failed to understand the current status of the electrical system and failed to followed procedures.

Perhaps the most the most obvious and unsettling observation from a PRA methodology point of view is that an event of this type is unlikely to survive probability-based screening of PRA. The large number of seemingly independent contributors would push the scenario to practically zero in a typical PRA.

Additionally the event highlights some important human performance features that are not captured by the way HRAs are done now. These include the fact that simulator training did not match actual plant response, Emergency Operating Procedures (EOP) were deficient in regards to verifying RCP seal injection, and command and control within the control room was poor. During the event crew supervisors were distracted from oversight of the plant including the awareness of major plant parameters. In addition, supervisors failed to properly manage the frequency and duration of crew updates/briefs during the early portion of the event leading to interruption in the implementation of emergency procedures and distraction the operators.

4.2 Fukushima Dai-ichi NPP Seismic/Tsunami Event

On March 11, 2011, the Fukushima Dai-ichi plant site was hit by the combined forces of a 9.0 magnitude seismic event and subsequent tsunami waves, more than 30 ft. in height, that flooded the site. Of the six reactors, Units 1-3 were operating at full power at the time of the event, while Units 4-6 were shutdown for maintenance. The units were designed to withstand magnitude 8.2 earthquakes and the seawall protecting the plants was design to withstand 20 ft. tsunamis. It appears that no serious damage was done to the reactors by the earthquake. The safety systems responded as designed to the seismic event, reactors were shut down automatically, and safety systems kicked in to remove the decay heat. All six external power sources were lost due to the earthquake, but the emergency diesel generators located in the basements of the turbine buildings started up.

The tsunami hit 55 minutes later. Tsunami waves submerged and damaged the seawater pumps for the main condenser circuits and the auxiliary cooling circuits including the Residual Heat Removal (RHR) cooling system. Flooding disabled 12 of 13 emergency diesel generators, the electrical switchgear, and batteries, resulting in station blackout. The 125-volt DC batteries for units 1 & 2 were flooded and failed, leaving them without instrumentation, control or lighting. Unit 3 had battery power for about 30 hours. The reactors were isolated from their ultimate heat sink, and all three cores largely melted in the first three days. Fuel coolant interaction produced hydrogen gas. Operators had to vent the hydrogen to secondary containment building where it exploded. The hydrogen explosion in Unit 4 escalated the severity of the event.

Major challenge facing the operators for weeks was restoring heat removal from the reactors and coping with overheated spent fuel ponds, an operation that involved hundreds of utility personnel, firefighters, and military. The site experienced hundreds of aftershocks, including an earthquake with magnitude 7.1, nearly a month after the initial 9.0 shock. After three weeks Units 1-3 were stable with water addition but no proper heat sink for removal of decay heat. Cooling with recycled water from new treatment plant was established in July, and reactors reached 'cold shutdown condition' in mid-December. In addition to complexities of providing heat removal, the responders faced the formidable task of preventing release of radioactive materials, particularly in contaminated water leaked from the three units. The accident response and evacuation were made extremely difficult due to road damage and obstructions. Over time more than 100,000 people had to be evacuated from their homes in an evacuation zone extended to 20 km. The accident was rated 7 on the INES scale.

Siu et al [6] list the set of potential PRA technology challenges identified posed by the events at Fukushima. These challenges involve phenomena or situations for which current PRA technology does not appear to be s s. They include:

Extending the PRA Scope: Potential risk significance of accidents triggered by regional events that could involve multiple sites, and possibility of release of radionuclides from multiple sources were evidenced by the Fukushima and concurrent events at other Japanese plants. This signifies the need to extend PRA scope to cover interdependent multi-unit risk exposure to a common external hazard, physical connections (e.g., unit cross-ties), the physical impacts of the events (e.g., explosions, radioactive material release), and accident response resource limitations.

Treating Feedback Loops: The delay in containment venting for Fukushima Dai-ichi Unit 1 caused by incomplete evacuation provides an indication that feedback loops and iterations may be needed among different levels of the PRA models, a departure form “once-through” approach used in current NPP PRAs, progressing from a core damage event (Level 1analysis) to containment response and source term assessment (Level 2 analysis) and then to offsite consequences (Level 3 analysis). Feedback may also be needed for example in multi-unit analyses where progression of risk scenarios in a unit may affect the progression of the scenarios in other units in terms of nature, severity and temporal sequencing of the events.

Reconsidering “Game Over” Modeling: “Game Over” modeling in typical PRAs relies on conservative simplifying assumptions to terminate the modeled accident scenarios early. For instance scenarios involving complete loss of power can be assumed to lead to core melt in a time scale much quicker than the times reported for Fukushima Dai-ichi Units 2 and 3. Such treatments not only miss the opportunity to identify and assess potentially effective accident management improvements, they also provide skewed input to the Level 3 analysis.

Treating Long Duration Scenarios: The tendency in PRA practice is to assume that in long duration scenarios (on the order of days and weeks) time is on side of safety and stability. More detailed and realistic treatment of such scenarios may reveal cases violating this assumption. Examples include changes in the external environmental conditions, such as earthquake aftershocks (at Fukushima Dai-ichi, earthquake aftershocks and tsunami warnings disrupted response to the initial shock and flooding), and interruptions in the availability of physical and social infrastructure and resources needed to cope with the accident, particularly when essential safety functions are provided by unconventional means.

Improving and Expanding External Hazards Analysis: This refers to the need for more refined external hazards analysis, including the consideration of both extreme hazards and concurrent failures, multiple correlated hazards (earthquake and tsunami in the case of Fukushima); multiple shocks (and warnings), multiple damage mechanisms (e.g., a tsunami analysis should, in addition to inundation, consider other effects such as dynamic loads from water and debris and clogging from debris)

Improving HRA: Response events at Fukushima

provide further evidence of the need for explicit treatment of errors of commission (e.g., the intentional isolation of the Isolation Condenser system at Fukushima Dai-ichi Unit 1), different decision makers (i.e., not the typical control room crew) who made potential errors in the prioritization of work, and potential psychological impacts on operators, advisers, and decision makers, recovery action feasibility and time delays, and the effects of long scenario duration (including fatigue, stress, and cumulative dose). New performance influencing factors may need to be included in HRAs to account for interruptions in response efforts due to external factors (at Fukushima Dai-ichi, earthquake aftershocks and tsunami warnings disrupted site operations as operators had to take shelter and then assemble for accountability), and the toll on operators. Other considerations include analysis of feasibility of operator actions performed outside the control room, in terms of adequacy of time, accessibility of the action location, and availability of staff with required skills. In the Fukushima event, some actions were significantly delayed because only contractors or other offsite personnel knew how to perform certain actions, and also because of environmental hazards such as seismic aftershocks, and radiation. An additional HRA challenge is modeling situation assessment with missing or misleading information due to for instance instrument failures, a likely scenario in post-core damage events. The guidance used in such scenarios (e.g., Severe Accident Management Guidelines – SAMGs) can call for a knowledge-based decision among a set of difficult choices.

4.3 Space Shuttle Columbia Accident

On February 1, 2003, Space Shuttle Columbia disintegrated during the reentry phase at the end of its mission, resulting in loss of its crew, grounding of Shuttle flights, and significant safety and operational impact on the International Space Station (ISS) among other consequences. The accident scenario as outlined by the Columbia Accident Investigation Board (CAIB) is as follows:

- 81 seconds after launch, at an altitude of 65,000 feet, Mach 2.46, bipod foam separates from the External Tank
- Foam, 21 to 27 inches long by 12 to 18 inches wide, weighing 1.67 pounds strikes the vehicle at relative velocity of ~545mph
- Foam impacts Wing Leading Edge Reinforced Carbon-Carbon (RCC), a part of the Shuttle Thermal Protection System (TPS) near Panels 8-9, creating a hole in the wing
- On re-entry, plasma enters the breached leading edge of the wing near Reinforced Carbon-Carbon Panels
- Plasma flow in left wing degrades internal structural integrity
- Vehicle motion too great for flight control system to manage, leads to loss of vehicle control and aerodynamic break-up

Other aspects of the accident scenario include the apparent decision that the observed External Tank foam impact during Columbia ascend did not cause significant damage based on experience from similar impacts in earlier flights, and the decision not to pursue the possibility of visual inspection of any potential damage.

For approximately two decades NASA sponsored a number of full and limited scope PRAs of Space Shuttle missions, with median probability estimates of loss of crew and vehicle (LOCV) ranging from 1/245 to 1/78 per flight. A number of these PRAs included a category of accident scenarios involving damage to the TPS due to de-boding of tiles or impact of orbital debris with a LOCV probability of about 2E-3, according to one PRA. The Columbia scenario in a very broad sense could be placed in this category although clearly the exact nature of the initiator and pursuing sequence of events are not identifiable in the lumped scenarios. Counting the Columbia accident, direct point estimate of the scenario probability (about 1E-2 per mission) is higher than, but not statistically inconsistent with the PRA estimates.

The Columbia accident has highlighted a number of deficiencies in PRA methodology as currently practiced for space missions. Three different categories are briefly examined here. A longer list of issues has been discussed elsewhere [7].

Columbia and other space mission accidents have also highlighted the significance of more detailed causal modeling. More accurate prediction of the nature (damage mechanism) of the Columbia accident initiator would have required a probabilistic physical model with consideration of aleatory uncertainties in the foam size, impact load, and RCC fragility. This would require re-tooling of the current PRA codes that have limited or no capability for integrating physical phenomena models. We note that extension of basic event probability models to include "physics of failure" may not be sufficient without adequate consideration of possible physical and stochastic dependencies of system failures due to the common underlying phenomena. While this type of interdependency has been recognized in modeling the impact of "external initiators" such as seismic, fire, and flooding events in NPP PRAs the current modeling and analysis platform imposes many restrictions that necessitate excessive simplification in modeling of the impact of such external events.

The actual sequence of events in the Columbia accident included several human decision points, rooted in cultural and organizational factors. The CAIB report has highlighted safety implications of a number of broadly classified organizational factors such as "reliance on past success," "organizational barriers to effective communications," "lack of integrated management," and "informal decision-making processes." Two interdependent examples are: (1) apparent assignment of low TPS damage probability based on past (but statistically insignificant) successes, i.e., negligible damage from foam and ice impacts during earlier

flight, and (2) the decision to continue normal mission activities without exploring possible rescue options.

These elements of the accident scenario can be easily overlooked in PRA accident scenario models when the decision making process, organizational factors and their paths of influence are not explicitly included. In fact even the methods currently proposed for incorporation of organizational factors into PRA do not explicitly address the potential for the direct impact of such factors on risk scenario branch points. Rather they attempt to enhance the causal models and probabilities of existing branch points and corresponding basic events, i.e., component failures and operator actions. An approach for explicit modeling of decision points in developing risk scenarios has been proposed.

Finally, compared with PRA estimated core melt frequencies for the US nuclear power plants (typically in the range 1E-5 to 1E-3 per reactor year), human space mission failures are far more frequent by several orders of magnitude. Estimation of such high probability risk events can be adversely impacted by some of the approximations routinely made in nuclear PRAs. One implication is that the use of nuclear PRA computer codes (e.g., SAPHIRE) that rely on probability truncations and other approximations for large models may be inappropriate for space mission PRA applications. We note that the technology currently exits (PRA codes using BDD-based algorithms [8] for cut set identification and quantification) removing the need for such approximations.

5. NEEDED IMPROVEMENTS WITHIN CURRENT PRA FRAMEWORK

The preceding discussions on strengths and limitation of the conventional PRA methodologies as practiced for instance in nuclear and space applications, and observations about the three accidents reviewed above, point to a number of methodological improvements that can significantly enhance the quality and credibility of PRAs. In summery we need

- Improved causal models at least for some applications (e.g., SDP). In some cases this means additional causal layers and introduction of more detailed models (including “physics of failure” models and models of organization factors) to support the quantification of the basic event probabilities and interdependencies. PRA is still very much hardware-oriented, while how a plant/system is organized and managed and the nature of its culture and safety attitudes can be are important risk contributors that need to be incorporated into PRA models. Equally important are use of more explicit modeling of system software and control failures and better integration of such failures into the process of structuring risk scenarios.
- Extended PRA scope to cover interdependent multi-unit and distributed systems risk exposure to a common external hazard, physical connections (e.g., unit cross-ties), the physical impacts of the events (e.g., explosions, radioactive material release), and accident response resource availability
- Improved and expanded external hazards analysis, including modeling of multi-hazard situations as well as better treatment of long duration events
- Tighter integration of the models three levels of PRA, better treatment of “feedback loops”
- Improved HRA, particularly use of causal modes for understanding of human response during an accident. Also a closer consideration of decision making with limited or misleading information (for instance for sever accident conditions), and more detailed models of possible complexities in carrying out tasks due to external factors.
- Use of advanced computational methods and solution algorithms (for example algorithms based on Binary Decision Diagrams) for increased accuracy and shorter processing time. This is important for applications that “rare event approximation” for probabilities could introduce significant errors, and cases where what-if analyses are needed to explore changes in risk profile by changing modeling assumption and postulating different conditions in the risk scenarios and their constituent events.
- Incorporation of lessons leaned and insights from previous events and accidents into PRA models and modeling process. This was one of the original objectives of precursor studies, which was never pursued in a systematic and consistent manner.
- Explicit inclusion of important "decision points" in risk scenario models (particularly at the event tree of event sequence diagrams levels). During major accidents “closed” systems quickly become open systems. Causes and consequences often go beyond the physical and organizational boundaries of the system. Command and control and decision-making can change, sometime chaotically. Current PRAs tend to limit modeling of decisions and interventions to those made by system operators. However, response to a system accident may involve other actors such as managers of the organization, or other decision makers outside the system (for example regulatory bodies, emergency response organizations, and public officials). Such decisions can significantly alter the sequence of events and could become major contributors to the risk.
- Better use of the computer power now available in extracting qualitative information from PRA models. There is a wealth of information in the millions or even billions of scenarios that can be created using PRA models, and computers today are able to sort, search, characterize, and categorize them to highlight

hidden complexities and vulnerabilities that can be masked by probabilistic ranking and screening of scenarios.

6. BEYOND CURRENT FRAMEWORK

Some of the main limitations of the classical PRA framework are:

- Risk scenarios and system vulnerabilities are essentially developed by the analyst, meaning that the PRA methodology itself does not "discover" the scenarios, rather it is to a large extent a way of documenting and organizing the analyst's discoveries
- Identifying risk scenarios in case of highly complex, dynamic, hybrid systems of hardware, software, and human components is very difficult, if not impossible, with the static, largely hardware-oriented classical framework
- Binary logic and deterministic cause-effect constructs that are at the core of fault tree/event tree techniques limit the spectrum of real world risk causal factors of that could be included in risk scenarios

To address these limitations new modeling approaches and computational algorithms have been developed or are being explored by researchers. The emerging methods can be categorized and "evolutionary" (by extending current PRA framework but not the fundamental style and modeling paradigm), and "revolutionary" (by totally changing the way risk models are developed, integrated, and analyzed). In the following we briefly describe prominent techniques under these categories, more specifically the hybrid causal logic (HCL) methodology and simulation-based or dynamic PRA methods

6.1 Hybrid Methods

Hybrid methods refer to integration of different modeling techniques for developing risk scenarios and contributing causes. With this definition classical PRA framework is also a hybrid method, mixing deductive and inductive logic models (event trees and fault trees). But both the event tree and fault tree techniques are essentially binary logic models representing deterministic logic links among constituent elements (basic events). The emerging hybrid methods tend to mix fundamentally different representational and computational techniques. Examples include:

- Logic-based simulation (DFM) [9]
- Linked Non-binary Event Sequence Diagram and Fault Trees
- Linked Fault Tree and Markov Models (to localized systems dynamics) [8]
- Hybrid Causal Logic (HCL) Method [10]

The HCL methodology extends the deterministic causal logic (ETs and FTs) of traditional PRA models to include ''soft'' factors, such as the organizational and regulatory environment of the physical system. The integrated hybrid causal modeling framework is composed of three layers: ESDs form the top layer, FTs form the second layer, while Bayesian Belief Networks (BBN) form the bottom layer. An ESD is used to model temporal sequences of events at a relatively high level of abstraction. In the second layer, fault trees are used to model the factors contributing to the properties and behaviors of the physical system (e.g., hardware, software, environmental factors). In the third layer BBNs extend the causal chain of events to potential human, organizational, and socio-technical roots where the causal relationships are often of uncertain and non-deterministic nature. Since the impact of human and organizational factors are usually shared by similar and dissimilar components, their inclusion via BBN linked to multiple system FTs properly accounts for dependencies emerging form the common causal factors in a natural and explicit way. The HCL solution algorithm, a hybrid of the BBN solution algorithm and Binary Decision Diagram (BDD) algorithm is capable of finding "cutsets" of the hybrid model HCL ("most likely contributing states"), calculated Importance Measures, and propagate uncertainties in probabilities of the hybrid model elements and links. A comprehensive HCL-based PRA platform (IRIS) has been developed and used in several important applications, most notably for civil aviation safety oversight and risk management. [10]

6.2 Simulation Based Methods

Simulation Based PRA methodologies (also known as Dynamic PRA, DPRA) are essentially model-based simulation approaches for generating risk scenarios. To do so, rules of stochastic and deterministic behaviours of the system and its elements (hardware, software, human operators, process variables, and environmental conditions) are developed as building blocks of a computer simulation platform. The simulation platform tracks possible changes in the states and values of the elements of the system as a function of time. By accounts for the nature and impact of the interactions and interdependencies among the system elements, risk scenarios are generated by a simulation engine. Depending on the particular method chosen for scenario generation, probabilities of individual or clusters of scenarios are calculated for the system "end states" of interest. Dynamic methodologies are particularly powerful when the system includes control loops, and/or complex hardware/process/ software/human interactions. They provide a natural environment to include physical models, such as thermal hydraulic codes for NPPs, and physics of failure models for hardware failure, as well as the impact of natural hazards events.

Dynamic PRA methodologies fall into two main categories: continuous-time methods, and discrete-time methods. Many of the research tools in the DPRA domain

have adopted the latter. In this style of simulation, scenarios are generated by branching to new sequences based on changes in the states of the system elements and variables, at user-specified time intervals. For each scenario, a time dependent probability is calculated based constituent branch probabilities [11].

Dynamic simulation-based approaches offer several key advantages over the traditional "static" FT-ET based PRA method. For example, dynamic simulation approaches can more realistically represent event sequence timing, provide a better representation of thermal hydraulic success criteria, and permit more detailed and realistic modeling of operator response.

Furthermore in DPRAs much of the complexity of enumerating scenarios is delegated to scenario generating algorithms, with reduced analyst-to-analyst variability of the results as an added benefit. DPRA allows heterogeneous models of various phenomena to be devolved and used at different levels of detail. Simulation tracking can provide desired information on nature of scenarios ("white box" simulation). To cope with the possible "scenario space" exploration, smart algorithms have been explored for produce dominant risk scenarios at reasonable simulation time. These include advanced Quantitative Biasing (biased sampling), and Qualitative Biasing or "simulation planning". Examples of DPRA platforms are ADS [12] and ADAPT [11]

Dynamic PRA however has its own challenges as outlined by [13]

- Development of physical models can be resource intensive and validation/accreditation of models can be difficult, particularly for rare events
- Obtaining a complete risk profile, i.e., ensuring that a complete solution space is examined and representative samples are chosen still requires further research
- Methods are needed for aggregating, interpreting, and communicating results. Simulation-based approaches can produce expansive amounts of data and as such identifying and focusing on key accident scenarios can be difficult
- Efficient method are lacking for uncertainty analysis as certain types of uncertainty and variability can actually alter the structure of risk scenarios as they evolved over the time.

Despite these challenges Coyne et al [13] see some near term benefits for regulatory applications including:

- Event and condition assessment (for cases involving complex dependencies and success criteria, degraded equipment, and variability in human response)
- Support in expert elicitation/expert judgment based decision-making. Simulation Based PRA can provide useful insights and benchmarks for expert judgment process (plant response, accident phenomenology), and help establish a narrative of accident scenarios
- Insights to support traditional PRA modeling. DPRA is a natural platform to combine probabilistic and deterministic modeling approaches, in developing success criteria, identifying causes, forms, and consequences of human actions, and in structuring event trees. It can also help foster better understanding of the consequences of uncertain assumptions in conventional PRAs.

7. CONCLUDING REMARKS

We have discussed some the strength and limitations of the conventional PRA methodologies as used in some technological sectors primarily nuclear power industry, space, and aviation. A number of methodological improvements that can significantly enhance the quality and credibility of PRAs have also been listed. While current methods will remain adequate for certain problems, the next generation of PRA methods and tools are likely to be hybrid methods and simulation based approaches.

Main drivers of this evolutionally path are

- Expanding domain of applications of risk-informed methods including risk-informed design and risk-informed emergency response. Such extensions require higher resolution of risk models, covering wider spectrum of causal factors, and more advanced inference and estimation methods
- Inadequacy of classical framework for modeling highly context-dependent events such as human errors, software failures, and dynamics of phenomenological events
- Need for improving stakeholder confidence in risk-informed decisions through improving and demonstrating credibility of PRAs. This is particularly challenging since in many direct Experimental validation not possible in most cases, and the fact that various benchmark studies on PRA method have revealed significant differences in results when the same risk problem is analyzed by different methods and/or different analysts

Some of the enablers of the trend towards improved PRA methods and introduction of new approaches are:

- Advances in modeling of socio-technical systems
- Advances in logic model solution algorithms and probabilistic inference methods
- Exponential increase in computational power, new data mining and visualization methods, and advancements in information sharing technology that can be sued for large scale collaborative modeling and analysis
- Rapid increase in use of "modeling and simulation" in engineering of complex systems, and opportunity that related tools and techniques can be used for full scale simulation-based risk analysis.

REFERENCES

[1] Reactor Safety Study, Nuclear Regulatory Commission, WASH-1400, 1975.

[2] Zion Nuclear Power Station Probabilistic Risk Analysis, PLG Inc. and Consumers Power, 1981.

[3] Indian Point Nuclear Power Station Probabilistic Risk Analysis, PLG Inc. 1981.

[4] Science Applications International Corporation, Probabilistic Risk Assessment of the Space Shuttle, 1995

[5] Ali Mosleh, N. Siu, C. Smidts, and C. Liu (Eds.) Model Uncertainty: Characterization and Quantification, University of Maryland Center for Reliability Publication, 1995.

[6] Nathan Siu, Don Marksberry, Susan Cooper, Kevin Coyne, Martin Stutzke, "PSA Technology Challenges Revealed by the Great East Japan Earthquake," PSAM Topical Conference in Light of the Fukushima Dai-Ichi Accident Tokyo, Japan, April 15-17, 2013

[7] Ali Mosleh, "Space Shuttle Columbia and PRA Methodology," Annual Meeting of the Society for Risk Analysis, Baltimore, Dec 7-10, 2003.

[8] William Vesely, "Fault Tree Handbook with Aerospace Applications," NASA- Prepared for NASA Office of Safety and Mission Assurance, August, 2002

[9] Houtermans, M.J.M., Apostolakis, G.E., Brombacher, A.C. & Karydas, D.M. (2002). The dynamic flowgraph methodology as a safety analysis tool : programmable electronic system design and verification. *Safety Science*, *40*(9), 813-833

[10] Katrina Groth, Chengdong Wang, Ali Mosleh "Hybrid causal methodology and software platform for probabilistic risk assessment and safety monitoring of socio-technical systems" Reliability Engineering and System Safety, 95(2010) 1276-1285

[11] Tunc Aldemir et al A Benchmark Implementation of Two Dynamic Methodologies for the Reliability Modeling of Digital Instrumentation and Control Systems, Office of Nuclear Regulatory Research U.S. Nuclear Regulatory Commission, NUREG/CR-6985

[12] Chang, Y.H.J. and A. Mosleh, "Cognitive Modeling and Dynamic Probabilistic Simulation of Operating Crew Response to Complex System Accidents -- Part 5 Dynamic Probabilistic Simulation of IDAC Model," Reliability Engineering & System Safety, 2007, 92(8): 1076-1101.

[13] Kevin Coyne and Nathan Siu, "Simulation-Based Analysis for Nuclear Power Plant Risk Assessment: Opportunities and Challenges" Proceeding of the ANS Embedded Conference on Risk Management for Complex Socio-Technical Systems, Washington DC, Nov 2013