

Technical Opinion Paper¹

Dynamic PRA for Nuclear Power Plants: Not If But When?

N. Siu

Abstract

This paper, which is aimed at NRC staff, provides my views on the promise, current status, challenges (technical and otherwise), and near-term path forward for dynamic PRA at the NRC. It also provides some cautions to prospective reviewers of a dynamic PRA, and numerous references for readers interested in more information. The purpose of the paper is to help NRC staff: a) develop an improved understanding of dynamic PRA, and b) formulate potential future activities in the area.

1. Background and Objective

In the context of nuclear power plant (NPP) PRA, “dynamic PRA” is a form of PRA in which driving forces on modeled plant elements and the element behaviors resulting from these forces are explicitly modeled over time [1].^{2,3} Originally developed to explicitly incorporate dynamic models for physical quantities (mass, momentum, energy) and control signals into a PRA [2-5], often in connection with fast reactor applications, the concept of dynamic PRA was later expanded to include other drivers, notably motivators and moderators (influencing factors) for control room crew decision making, both static (e.g., procedures, training) and time-dependent (e.g., information on current situation, stress levels) [6-7]. Nowadays, the term is generally used to refer to NPP PRA approaches that simulate system behavior and accident scenario development over time, whether or not driving forces are explicitly modeled.⁴ Other terms referring to same or closely related concepts are “Integrated Deterministic-Probabilistic Safety Assessment” (IDPSA) [8], “Integrated Safety Assessment” (ISA) [9], and “Computational Risk Assessment” [10].⁵

¹ This paper is written from the perspective of a former researcher and continuing supporter of dynamic probabilistic risk assessment (PRA). The views expressed in the paper are, of course, based on my own experiences and don't necessarily reflect those of the U.S. Nuclear Regulatory Commission (NRC) or even of others in the dynamic PRA or broader technical communities.

² It is important to recognize that current event tree/fault tree PRA models don't ignore scenario dynamics. The difference between a dynamic PRA and a conventional PRA is that the former will explicitly model the behavior of a system over time. See [Appendix B](#) for some examples.

³ Note that the term “dynamic PRA” can also be read as meaning a PRA that changes over time (e.g., as a risk monitor or a “living PRA”). As used in the PRA community, “dynamic PRA” is a shorthand term for the dynamic analysis discussed in this paper.

⁴ From this more general perspective, it can be seen that phased mission modeling approaches, in which the passage of time is treated implicitly through a series of quasi-static stages (e.g., as considered in a low power and shutdown – LPSD – analysis), might be considered a form of dynamic PRA. However, the focus of this paper is on methods where time is treated explicitly.

⁵ The term “computational risk assessment” emphasizes the point that simulation modeling relevant to PRA need not be confined to time-dependent processes. For example, it envelopes simulation approaches to physics-of-failure analyses (e.g., for passive component reliabilities or for common cause failure parameters).

Dynamic PRA has been topic of interest in the academically-oriented advanced PRA methods community for many years. Perhaps the earliest workshop was held in the mid-1980s [11]. Currently, at typical international PRA conferences,⁶ multiple technical sessions are devoted to the latest developments, and multiple journal papers and books have been written (e.g., [1, 12, 13]).

The NRC supported early dynamic PRA development efforts [6] through university grants to the Massachusetts Institute of Technology (MIT) and more recent studies at Sandia National Laboratories (SNL) [14] and the University of California at Los Angeles (UCLA). The U.S. Department of Energy (DOE), through its Light Water Reactor Sustainability Program's (LWRS) pathway on Risk-Informed Safety Margin Characterization (RISMC) at the Idaho National Laboratory (INL), is making a significant investment in software and model development, designed for U.S. industry use [10, 15]. SNL has also continued to work on developments [16-17]. As evidenced by international surveys on the use and development of PRA [18] and by numerous papers at recent PSA and PSAM conferences, a number of international governmental organizations (e.g., the European Union – EU, Spain's Consejo de Seguridad Nuclear – CSN), industry organizations (e.g., Electricité de France – EDF, the Nordic PSA Group – NPSAG), and technical support organizations (e.g., Germany's Gesellschaft für Anlagen und Reaktorsicherheit – GRS) are continuing to fund development work on dynamic PRA and IDPSA.

Despite the considerable interest and effort, the tools developed by ongoing activities are not, to my knowledge, being used to support current U.S. NPP decisions.⁷ This paper provides a brief summary of the reasons for continuing interest in dynamic PRA, potential pitfalls associated with its practice and use, and the status of the field. It then provides some cautions for reviewers of dynamic PRAs, and concludes with some personal opinions regarding where the field is headed and why the NRC should consider preparing for a future that includes dynamic PRA.

2. The Technical Promise and Allure of Dynamic PRA

From a technical viewpoint, dynamic PRA is a very attractive concept. As discussed below:

- it has the potential to increase PRA realism, e.g., through addressing important but as-yet unsolved problems (e.g., the systematic identification and treatment of cognitive and team behaviors leading to errors of commission);

⁶ Notably the American Nuclear Society's Probabilistic Safety Assessment ([PSA](#)) conference series, the Probabilistic Safety Assessment and Management ([PSAM](#)) conference series organized by the International Association for Probabilistic Safety Assessment and Management (IAPSAM), and the European Safety and Reliability ([ESREL](#)) Conferences organized by the European Safety and Reliability Association (ESRA). In addition to technical papers, some of these conferences have hosted workshops dedicated to dynamic PRA methods and tools.

⁷ Note that the offsite consequence analysis of a Level 3 PRA is a form of dynamic PRA, and that Level 2 analyses can use an accident progression modeling framework more akin to dynamic PRA than Level 1 analyses. Of course, Level 2 and Level 3 analyses played a role in early risk-informed regulatory decisions, including the 1983 Commission decision to allow continued operation of the Indian Point plant [19]. Note also that, in my view, performance assessments performed for geologic waste repositories are dynamic PRAs.

- it is consistent with the increasing use of simulation-based methods in engineering (and associated education and training of new engineers); and
- it provides a natural, holistic analysis framework that can facilitate the interaction and input of the multiple scientific and engineering disciplines engaged in a PRA, and the use of the PRA by non-PRA specialists.

For these reasons and others (discussed below), the subject is also inherently attractive to the research community. Of course, there are also downsides. Key challenges to fully integrated dynamic PRA modeling are discussed in [Section 3](#).

Before discussing the attractions in more detail, it is important to recognize the following:

- Conventional event tree/fault tree-based PRA models that are suitable for practical risk-informed applications certainly consider scenario dynamics. Various time-dependent phenomena and model element interactions are treated explicitly or implicitly in a number of areas. Examples include: thermal-hydraulic (T-H) success criteria modeling, fire scenario analyses (modeling of fire growth, suppression, and plant response), the modeling of time-critical human actions (including the recovery of offsite power following a loss of offsite power – LOOP, as well as various main control room operator actions), and post-core damage severe accident behavior. Bley et al. [20] provide a useful discussion on the treatment of timing in a conventional NPP PRA framework.⁸
- The term “dynamic PRA” is widely viewed within the PRA community as implying a highly detailed and complex analysis of the system of interest, and this is the view that drives ongoing discussions about the viability of dynamic PRA. However, a dynamic PRA need not always be complex or require sophisticated tools. [Appendix B](#) provides an example of a situation (recovery of emergency power following a LOOP) involving multiple, interacting entities and processes that can be analyzed via a simple object-oriented simulation. Such a modeling approach has long been considered routine by the simulation modeling community and multiple tools are available for implementation.⁹

2.1. Improving PRA Realism

2.1.1. *On Realism*

For the PRA enterprise, where analyses need to deal with highly unlikely events for which empirical data are sparse or even non-existent, the notion of “realism” is admittedly a squishy

⁸ In this paper, I use the term “conventional PRA” to refer to the event tree/fault tree analyses used in current NPP PRAs. Other terms in the literature include “classical PRA” and “static PRA.”

⁹ Information on the current state of simulation modeling can be found at the annual Winter Simulation Conference (e.g., [WSC 2017](#)). Roberts and Pegden [21] and Goldsman et al. [22] provide summaries of the history of the field; many of their observations concern the general practice of modeling and are directly relevant to PRA.

topic. Consistent with recent discussions on fire PRA maturity and realism [23], I consider realism as the degree to which, *as judged by the informed technical community*, an analysis represents the technical and organizational system relevant to the decision problem.¹⁰

From this perspective, any analysis approach that reduces modeling approximations and more faithfully represents the technical community's understanding of how things work (and fail) increases realism. Thus, for example, a dynamic PRA approach that does not need to define mission times and success criteria,¹¹ should, as least philosophically, be more realistic than a conventional PRA, which requires such intermediate modeling constructs.

Perhaps more important than the ability to reduce modeling approximations, dynamic PRA has the capability to improve current treatments of potentially important dependent failures, a matter central to the realism of a PRA. For example, as discussed below, dynamic PRA can enable direct analyses of FLEX strategies, more realistic analyses of external hazards, and can provide a rational approach to current PRA gaps, notably the treatment of passive safety systems and of so-called "errors of commission" involving intentional termination or bypass of safety systems.

2.1.2. Analysis of FLEX Strategies

Once the decision has been made to use FLEX equipment in efforts to prevent or mitigate a severe accident, the implementation of FLEX strategies involves multiple actions outside of the control room. The times required to perform these actions, some of which might need to be performed in sequence and others in parallel, are aleatory variables. Moreover, various events during implementation (e.g., successes and failures of sub-actions, decisions to shift implementation strategies and associated resources) are also aleatory. This problem appears to be naturally suited to dynamic analysis using currently available simulation tools. Note that Paris et al have recently performed a more sophisticated dynamic PRA analysis of the impact of FLEX on the risk associated with a loss of feedwater sequence, considering the plant T-H response as well as the times required to perform procedurally-directed actions [27].

¹⁰ In his 2003 speech "Realism and Conservatism," then-NRC Chairman Diaz defined the term "realistic" as "being anchored in the real world of physics, technology and experience" [24]. In a PRA context, because a) the PRA needs to deal with rare (and hopefully unobserved) events, and b) the ultimate purpose of practical PRA is to support decision making, it seems appropriate to tie the notion of "realism" to the needs of decision making.

¹¹ For example, in a simulation-oriented dynamic PRA, continuous processes (e.g., decay heat production and removal) are treated using phenomenological models. Such matters as cooling pump output and runtime need not be translated into "success" or "failure" states. Should the ultimate system outcome need to be characterized in terms of a discrete state (e.g., core damage), this can be done at the end of the analysis. Note that there has been considerable exploration of success criteria, at least for Level 1 PRA for operating reactors. (See, for example Corson et al. [25].) In a dynamic PRA context, CSN has supported a number of success criteria analyses. One recent study investigated the effect of different loss of coolant accident (LOCA) break sizes within the break size ranges used by a conventional PRA for a 3-loop pressurized water reactor (PWR) [26].

2.1.3. External Hazards PRA

As recently illustrated by INL-produced animations of hypothesized external floods [28],¹² physics-based hazard simulations can provide time-dependent challenges to the plant, and dynamic PRA methods provide a natural means for addressing associated issues (e.g., risks from scenarios involving progressive losses of equipment vs. those involving immediate loss, correlation between components and even units) [28]. Less dramatically, a recent review of past actual flood and storm events has highlighted the importance of flood timing to plant response [30], and it appears that a simpler dynamic PRA that accounts for possible differences in arrival times of different threats (e.g., wind vs. flooding) could be helpful for operational planning. [Appendix C](#) provides additional discussion on this potential application.

2.1.4. Passive Safety Systems Reliability

Passive safety systems play a major role in most new and advanced reactor designs. The expectation is that by eliminating the need for external power, system reliability will be improved over that of conventional, forced-flow systems.

It is well recognized that passive systems are engineered systems and are not perfect – there are scenarios where the systems will not function as intended. Conventional PRAs can readily treat some scenarios, e.g., when gravity-driven flow from a tank is blocked by a closed isolation valve. However, although there have been some limited studies of the impact of T-H uncertainties (e.g., see Pagani et al. [31]¹³), it appears that there has yet to be a detailed quantitative risk assessment of more complex situations, e.g., those involving significant departure from design T-H conditions, such as 3-D flow instabilities or even flow reversals. The extremely low risk estimates being produced by some new/advanced reactor PRAs naturally lead to questions regarding the risk importance of system conditions not explicitly modeled by the PRA. A structured investigation to determine whether such conditions could be noticeable contributors to the plant risk profile seems warranted.

Since it can include complex T-H models as an integral part of the analysis, dynamic PRA provides a natural approach for performing such an investigation. Furthermore, it appears that the required tools (e.g., computational fluid dynamics codes, probabilistic frameworks to exercise these codes under varying conditions, advanced methods to develop simplified “surrogate” models as needed [32], and post-processing tools to develop insights from the computational results) are available. Note that if such a study is intended for actual decision support (as opposed to a demonstration of methods), it would likely require involvement of a number of technical communities and significant resources.

¹² The videos were produced as products of research supported by the U.S. Department of Energy. Prescott et al. [29] provide representative still frames from the videos. Some videos are publicly available at <https://safety.inl.gov/public/>.

¹³ This study uses a simple, quasi-steady one-dimensional (1-D) model of a hypothetical gas-cooled fast reactor to investigate the impact of uncertainties in various model parameters, including power, pressure, wall temperature, and Nusselt numbers. System failure is defined based on material considerations (e.g., high temperatures that lead to high thermal stresses in system components).

2.1.5. *Errors of Commission*

All three of the major nuclear power plant accidents experienced to date involved errors of commission. At TMI 2, operators throttled high-pressure makeup. At Chernobyl 4, operators disabled the automatic reactor scram signal. At Fukushima Dai-ichi 1, operators isolated the passive isolation condenser. All three actions were not “random events” – they were human failure events (HFE)¹⁴ driven by a number of factors including crew training and situation context, and in all three cases, the situation context included the dynamic behavior of the plant, before (in the case of Chernobyl) or during (in the case of TMI and Fukushima) the accident.

The treatment of such errors continues to be one of the grand challenges for current human reliability analysis (HRA) methods. By providing a framework for integrating models for: a) plant thermal hydraulics, b) plant hardware (including instrumentation and control), and c) operating crew behavior (including cognition and teamwork), dynamic PRA directly addresses the operational context for crew decision making and action, and offers the promise of systematically addressing perhaps the most important, long-standing source of “completeness uncertainty” in current PRAs [33]. The technical difficulty in fulfilling this promise has been one of the drivers for dynamic PRA research and development (R&D).

2.1.6. *Additional Remarks*

It should be recognized that whether improved realism is needed naturally depends on the decision problem at hand. In this regard, “game over” modeling assumptions that conservatively ignore dynamic behavior (e.g., the increase in time available for operators to perform needed actions due to decay heat removal from a pump that operates for only a fraction of its full mission time) can be sufficient for the needs of system design or decisions regarding post-event regulatory response. On the other hand, the bottom-line results from such an approach might discourage the preparation and optimization of contingency plans preparing for such real-world situations.¹⁵ Furthermore, overuse of such simplifying assumptions can reduce stakeholder confidence in the realism of the PRA and hurt the ultimate practice and use of PRA.

2.2. Consistency with Current Directions in Science and Engineering

Although papers on the subject tend to be written by advocates, it seems clear that scientists and engineers are making increasing use of detailed computer-based simulation modeling to predict system behavior. These efforts, enabled by ever-improving computational infrastructure (software as well as hardware) can, in principle, lead to improved results and insights through the elimination of approximations required by simpler modeling approaches. In their most general, software-encoded form, simulation models can be developed to incorporate arbitrarily complex considerations (e.g., detailed phenomenology, non-linearities, rule-based interactions

¹⁴ The term “human failure event” is used in the HRA community to avoid the connotation that the failures modeled are necessarily the fault of the operators.

¹⁵ Note that a scenario that is a small contributor to such metrics as core damage frequency (CDF) might still be important to a plant from an enterprise risk management (ERM) perspective [34].

of model elements) should these be judged important to the analysis. (Cautions in assuming improved realism from increased modeling detail are discussed in [Section 3](#) below.) Further, as discussed in the following section, simulation modeling enables a “natural language” approach in which the modeler can focus on more literal representations of modeled elements and their behaviors, reducing the need for modeling abstraction. Advocates claim that simulation modeling “has advanced as a tool of choice for operational systems analysis” [22] and that it “does not require mathematical or statistical sophistication for model development and use” [21].

Dynamic PRA, as currently being pursued in the NPP PRA R&D community,¹⁶ is a particular form of simulation modeling that accounts for the special needs of PRA, including the treatment of rare events, phenomena affecting important dependencies, and uncertainties. As such, it is a problem solving approach that is consistent with the above trend in science and engineering. It can, therefore, benefit from developments not necessarily limited to the PRA community. These include: a) incoming analysts trained (e.g., from classroom education and research projects) to think in terms of simulation modeling, and b) ongoing activities in the broad scientific and engineering community aimed at improving simulation modeling practices, tools, and infrastructure [36].

2.3. Natural-Language Framework

Current dynamic PRA approaches, being simulation-oriented, encourage direct, phenomenologically-oriented modeling of the processes involved. If the time-dependent behavior of reactor system pressures, temperatures, and inventory are important, T-H models can be used. If the operating crew decision making in response to plant behavior is important, models for the crew cognitive behavior (including information detection, situation assessment, decision making, and execution) can be added.

In this approach, the behavioral models, which are developed using modeling frameworks and terminology natural to the relevant subject domains, need not be immediately converted into success/failure models. These latter discrete-logic models are well understood by the PRA community, but may not be the natural problem representation for other technical communities.¹⁷ In addition to the modeling efficiencies from allowing subject matter experts to use their normal modeling approaches, a simulation-oriented approach should improve the experts’ understanding of how their processes and expertise feed into the integrated PRA (and therefore the decisions supported by the PRA), and could increase their ownership of the PRA and subsequent buy-in to risk-informed decision making (RIDM) initiatives.

¹⁶ Generally speaking, current ADPRA approaches involve dynamic event trees – event trees that track discrete system changes over time – or some form of direct simulation (e.g., combined discrete-event and continuous simulation) [1, 12, 13]. Direct simulation techniques appear to be favored for complex problems outside of the NPP PRA arena. Devooght and Smidts have developed an elegant, PRA-relevant mathematical formalism to represent the dynamic behavior of stochastic systems [35]. However, Monte Carlo simulation methods are used to solve the differential equations of interest.

¹⁷ Even within the PRA community, it’s worth noting that some continuous, non-threshold processes important to non-light water reactor designs, e.g., the release of radionuclides from overheating fuel in a high-temperature gas reactor (HTGR), have given rise to arguments about the definition and utility of such basic concepts as “core damage.”

It is also worth noting that dynamic PRA:

- readily supports chronologically-oriented narratives (“stories”) of important scenarios that facilitate understanding of PRA results by non-experts (and even experts);¹⁸ and
- has the potential to make better use of operational experience, since the constituent sub-models in a dynamic PRA can benefit from potentially rich empirical information on behaviors during incidents beyond occurrence times and/or “successes” or “failures” of key events and actions.¹⁹ Given the rarity of challenging incidents and accidents, approaches that facilitate data mining should benefit the PRA/RIDM enterprise.

2.4. Technological Allure

Although I haven’t done any formal surveys, it’s clear that dynamic PRA is an exciting topic to PRA researchers inside and outside of academia. Despite a general scarcity of funding over the years (the previously mentioned activities at INL, SNL, and EDF are relatively recent developments), notable research programs (including those at the Ohio State University – OSU, the University of Maryland – UMD, UCLA, and GRS) have found ways to continue their activities.^{20,21}

Based on personal experience, the possible reasons for this attraction range from the idealistic (e.g., the promise of increased realism; the chance to do something new; the chance to make fuller use of non-PRA engineering education and tools), through philosophical (e.g., a preference for mechanistic rather than statistical modeling), to pragmatic (e.g., the ability to differentiate research from what’s been done in the past for purposes of academic advancement; the development of skills that are likely useful in a simulation-headed world, considering trends in the financial and entertainment industries as well as science and engineering²²).

Regardless of the reason, the attractiveness of dynamic PRA is important because it influences the direction of leading PRA R&D programs and, therefore, the specific research products that

¹⁸ The use of chronologically-oriented narratives to explain the PRA model is well-recognized in the broad PRA community. See, for example, the discussions of sequences in the NUREG/CR-4550 companion reports to NUREG-1150 [37].

¹⁹ For example, during the 1985 loss of feedwater incident at Davis-Besse [38], the plant operators decided not to implement procedurally-directed “feed-and-bleed” cooling, not only because they were reluctant to contaminate the containment, but also because they believed they could restore auxiliary feedwater in time. (And, as events showed, they were correct.) A dynamic PRA that models operator decision making can directly include these considerations.

²⁰ The lack of significant applications over the long time period since its inception is sometimes used as an indictment of dynamic PRA. It should be recognized that this is a “Catch 22” situation – the lack of continuing investment by near-term oriented R&D sponsors has led to shoestring activities at universities, and therefore academic-level demonstrations of potential that spark little interest by sponsors who are also responsible for maintaining current PRA tools. Recent, DOE-sponsorship of larger-scale activities might break this cycle.

²¹ Note that the CSN’s long-term collaboration with dynamic PRA researchers at the Universidad de Politécnic de Madrid (UPM) appears to be a counter-example to the general approach (until recently) of funding agencies.

²² For example, in 1997, the National Research Council, recognizing the similarities between video games and military simulations, held a workshop involving the entertainment industry and the defense R&D community [39].

NRC might wish to leverage. Furthermore, it can affect the problem-solving approaches and cultural attitudes of students entering the PRA community. Regarding the latter, if NRC is viewed as a guardian of the “tried and true” and an impediment to the new, this can hurt the recruitment of top students. To the extent that contractor staff preferences can affect the staffing of NRC-sponsored projects, graduating student attitudes might also eventually affect NRC activities.

3. Status and Challenges

3.1. Status of Dynamic PRA

As discussed earlier in this paper, “dynamic PRA” can be considered as a broad class of methods within the even broader class of simulation-based analysis methods. The general field of simulation modeling is mature.²³ Task-oriented simulation tools have been used to inform crew manning decisions for advanced warship designs considering the demands of battle [40], and are being proposed for use in “right-sizing” security forces for NPPs.²⁴ The annual Winter Simulation Conferences²⁵ provide a good sample of the wide range of simulation applications currently being pursued.

Regarding applications intended for NPP PRA, there are a wide variety of techniques and tools with varying levels of technical maturity. At one end of the spectrum, fully mature, network modeling approaches (e.g., Markov models [41]) can be used for many systems, and general purpose simulation tools can be used to create useful models to address dynamic interactions between components, as long as such modeling doesn’t require explicit treatment of physical phenomena. (See, for example, [Appendix B.](#))

Some organizations are creating object-oriented simulation toolboxes that can be used to model somewhat more complex situations involving fairly simple phenomenological considerations, e.g., when the behavior of a process can be represented by a limited set of equations and constraints. The EDF PyCATSHOO tool [42], which is being used to support pre-conceptual design activities for ASTRID, a French Generation IV pool-type, sodium-cooled fast reactor design [43], falls into this category. However, such tools are not yet being routinely applied in NPP PRAs.²⁶

Dynamic PRA tools that fully integrate the behavior of plant hardware, physical phenomena, and operators are at the lesser end of the maturity scale. These tools are still under development at universities (particularly OSU, UCLA, UMD, joined by with some recent efforts at the University of Illinois Urbana-Champaign - UIUC), national laboratories (particularly INL and SNL), and

²³ See [Appendix D](#) for a set of indicators for technical maturity.

²⁴ A public discussion on relevant simulation tools was provided at an Institute of Nuclear Materials Management workshop in Boston in 2015.

²⁵ See Footnote 9.

²⁶ Per discussions with the developers, it appears that the physics involved in the ASTRID application are considered to be relatively simple by the modelers. More complex phenomenology, such as that demanding the use of a full T-H systems code e.g., MELCOR or MAAP), require a more complex tool than PyCATSHOO.

international organizations (e.g., CSN, EDF, GRS). (See Table 1 for summary information.) A number of significant, and often inter-related technical, economic, and socio-organizational challenges to the widespread, practical application of these advanced tools are listed below.

Some of the listed challenges are being resolved. Others may be self-resolving over time due to a variety of reasons, including new industry initiatives, the technical demands of new problems, general advances outside of the PRA community, and the changing makeup of the PRA community. On the other hand, some challenges may need effort by the PRA community as well as developers. It should also be recognized that unforeseen challenges will likely arise during if and when the tools are used in practical, decision-grade applications.²⁷

Table 1. Summary Information on Some Current Dynamic PRA R&D Programs

Organization	Principal(s)	Early Pubs. ^a	Current Tool(s)
Ohio State University	T. Aldemir, C. Smidts	1987	ADAPT [16, 17]
University of California at Los Angeles	A. Mosleh, ^b M. Diaconeasa	1993	ADS/IDAC [44, 45]
Universidad Politécnica de Madrid	E. Meléndez-Asensio ^c	1994	SCAIS [26]
Gesellschaft für Anlagen und Reaktorsicherheit	M. Kloos	2006	MC-DET [44]
Sandia National Laboratories	M. Denman	2008	ADAPT [16, 17]
Idaho National Laboratory	D. Mandelli, C. Smith	2013	RAVEN [45]
University of Maryland	M. Modarres, K. Groth	2015	ADS/IDAC [44, 45], ADAPT [16, 17]
Electricité de France	V. Rychkov	2015	RAVEN [45], PyCATSHOO [42]

^aDate of early publications found by a quick search; earlier publications are quite possible.

^bStarted at U. Maryland before moving to UCLA.

^cCSN Point of contact. Recent papers on ISA are typically authored by a large team of collaborators from UPM, CSN, and NFQ solutions. J.M. Izquierdo (CSN) was an early leader and continues to contribute.

3.2. Technical Challenges

Most of the following topic areas are being addressed by current dynamic PRA R&D activities, but some have not yet gained much attention. The starred items are particularly relevant to the concerns of reviewers of potential near-term applications and are further discussed in [Section 4](#).

- Realistic modeling of operator behavior (particularly cognitive and team behavior)
- Identifying, collecting, and appropriately using evidence for input parameters (considering potential dependencies)*
- Determining and performing appropriate verification and validation processes (including identification and treatment of out-of-bounds conditions)*
- Ensuring tools can be exercised using available computational resources
- Developing aids to support searches for potentially important conditions and scenarios*

²⁷ For example, WASH-1400 [48] took a highly simplified approach to common-cause failure modeling that was later criticized in the Lewis Commission's review [49], and it was prompted to include a quick and limited analysis of fire only after 1975 Browns Ferry fire.

- Developing effective methods and tools to help users make sense of voluminous and complex outputs with potentially large uncertainties, while avoiding unwarranted aura of high precision and accuracy*

3.3. Economic Challenges

Perhaps the greatest challenge to dynamic PRA developers arises from the success of conventional PRA modeling, and the consequent large base of models, practitioners, and users. Moreover, this base is supported by a substantial infrastructure (including software tools, standards, guidance, and training). To make economic sense, developers need to convincingly address the following basic challenges.

- Demonstrating that their dynamic PRA tool will provide added value to RIDM activities already informed by results and insights generated using current PRA tools; and
- Demonstrating that the required resources for practical tool use in decision support applications are likely to be acceptable.

3.4. Socio-Organizational Challenges

Over the years, many dynamic PRA developers and advocates have been frustrated and confused by the broader PRA community's unwillingness to adopt, even on a trial basis, what they consider to be a clearly superior approach. It appears that many in the broader PRA community, while accepting the possibility that dynamic PRA might indeed provide better information for some situations, are: a) skeptical regarding past dynamic analyses aimed at demonstrating value, and b) convinced that dynamic PRA is an excessively complicated enterprise. Of course, it's possible that such skepticism is partially fueled by an understandable reluctance to foster change in a working RIDM environment, especially when change requires additional resources with unproven benefit. In addition to the technical and economic challenges listed previously, a number of challenges regarding community perceptions and programmatic directions might need to be addressed to enable wide-scale adoption of dynamic PRA. These include the following.

- Changing the perception of dynamic PRA to recognize the wide variety of methods and tools available, many of which are mature and widely used outside the NPP PRA arena
- Changing mindsets within the dynamic PRA R&D community. This includes:
 - recognizing that in practice, increased modeling detail doesn't necessarily improve realism;
 - improving appreciation of the importance of insights (as opposed to bottom line risk results) in decision making; and
 - increasing openness to and understanding of the concerns raised by skeptics.
- Changing mindsets within the PRA user community. This includes:
 - increasing appreciation of the value of different modeling approaches; and
 - increasing awareness and appreciation of modeling trends and developments outside of the PRA community

- Improving the targeting of dynamic PRA development activities. This includes:
 - transitioning from an R&D activity to a product development activity (with associated development processes including formal requirements specifications and testing);
 - increasing emphasis on solving problems important to RIDM rather than those posing the greatest technical challenge;
 - deciding how dynamic PRA best fits in the PRA toolbox; and
 - determining what new technical expertise is needed to implement dynamic PRA and how this expertise should be developed and maintained.

Note that similar to the technical challenges, many of these challenges have been recognized and a number are being addressed.

4. Cautions to Reviewers

The preceding discussion addresses the performance of advanced dynamic PRA (ADPRA²⁸) in practical applications as an open question. Although this appears to be the general situation, it is important to recognize that the literature includes a few examples where dynamic PRA was apparently used support of actual advanced reactor designs. Some of these were performed in the early 1980s [3]; one of the most recent ones is ongoing [43]. In such a situation, of course, the prospective applicants have decided that ADPRA is worthwhile and, therefore, many of the economic and social challenges listed in [Section 3](#) are moot. However, there remain a number of important technical challenges important to reviewers.

The following discussion provides some initial points for reviewer consideration. Many of these points are based on theoretical grounds. I expect that as the PRA community gains practical experience with performing and reviewing decision-grade ADPRAs, better reviewer guidance can be developed.

4.1. Data and Model Parameter Estimation

Based upon current development directions, an ADPRA model is, in many ways, likely to be analogous to a deterministic model created using a T-H systems code such as TRACE, MELCOR, or MAAP. Thus, it will employ a large number of sub-models, many of which will employ parameters requiring user-supplied input. Ideally, this input will be in the form of probability distributions that quantify the parameter uncertainties. Some reviewer considerations are as follows.

- Similar to a conventional PRA model, the ADPRA model will likely include some parameters for which data are sparse (e.g., failures of analogous components under

²⁸ The dynamic PRA community readily introduces new terms (and associated acronyms) in attempts to draw distinctions among approaches. I reluctantly use the descriptor “advanced” in this paper only to emphasize my view that: a) dynamic PRA need not be complicated; and b) mature, relatively simple tools are available for some dynamic PRA analyses.

accident-like conditions), observable but not yet observed (e.g., times taken by plant staff to perform certain accident management actions), or not even directly observable (e.g., operator situation assessments given cues). Depending on the sensitivity of the ADPRA to the parameters (see [Section 4.2](#)), these data limitations may play an even more important role in the overall ADPRA results and uncertainties than in those for a conventional PRA. It may be even more important, therefore, to review the evidence used to estimate key sub-model parameters and how this evidence was used.

- Especially in situations where parameter uncertainties are not treated realistically,²⁹ a parameter's probability distribution might include values outside the range for which the sub-model is applicable. At least for key parameters, in addition to reviewing how available evidence was used to generate the input distributions and verifying the reasonableness of these distributions, the reviewer should check to see if the dynamic PRA model includes checks for out-of-bounds inputs.
- Related to the previous point, the sub-model parameters might be dependent due to underlying phenomenological relationships. For example, if a T-H model requires that heat transfer coefficients and friction factors be input rather than calculated, it should be recognized that these parameters are correlated through their dependence on the same fluid properties. In principle, therefore, a dynamic PRA might need to consider joint probability distributions for sets of parameters, rather than treating each parameter separately. Note that this issue isn't as esoteric as it may sound, as independent sampling of parameter values can lead to physically unrealistic or perhaps even impossible combinations. Parameter dependence might be an issue that the dynamic PRA R&D community hasn't spent much time on, and so problems are likely to be revealed only through anomalous results. A tool to independently test hypotheses regarding input data would likely be useful.

4.2. Verification and Validation

Given the analogy with deterministic T-H system codes, it seems that at least some aspects of ADPRA verification and validation (V&V) could be treated in a similar manner. Regarding verification (i.e., showing that the code does what it is intended to do), it seems that review procedures would be similar at least in nature, although an ADPRA verification review might need to be greater in scope due to ADPRA's treatment of uncertainty. Picoco et al. discuss the use of a software tool to support dynamic PRA model verification [50].

Regarding validation, recognizing the general lack of empirical data to "prove" that the model faithfully represents "reality" (see [Section 2.1.1](#)),³⁰ ADPRA reviewers might employ the approach used in T-H code reviews. This approach is aimed at determining a code's

²⁹ For example, using non-informative prior distributions in a Bayesian analysis is a pragmatic approach to avoid the effort required to express knowledge in terms of probability distributions, but will (by design) lead to distributions broader than those based on informative prior distributions.

³⁰ Note that data generated by the Halden HRA Empirical Study for a limited set of scenarios has been used to assess the ability of ADS/IDAC to reproduce key behaviors and events [51].

acceptability for use in specified applications, rather than validating the code. The acceptability determination is based on available evidence, including benchmark code comparisons.³¹

Whatever the term and the ultimate performance criteria used in the review, at least for early applications, it is important to consider both the general ADPRA model, as implemented by the software tool (“code”), as well as the NPP-specific model, as represented by user-supplied input. Some specific considerations are as follows.

- A fundamental difference between an ADPRA model and a deterministic systems model is that the former needs to include the possibility and probability of unlikely events.³² The reviewer needs to check to see if and how such events were identified and treated.³³
- As discussed in the preceding section, input parameter distributions can include values that are out-of-bounds for the ADPRA sub-models. The reviewer needs to check if and how the ADPRA code identifies and treats such conditions.
- Similarly, it isn’t unusual for deterministic sub-models in the ADPRA code to reach conditions where the code “hangs” (due to excessively slow numerical convergence). In general, ADPRA developers have recognized these possibilities and have developed workarounds (e.g., by stopping the affected simulation trial and counting the trial as a system failure). The reviewer needs to consider whether these workarounds significantly affect the ADPRA results and insights.
- It is well-recognized that ADPRAs are computationally intensive, and considerable efforts have been taken to develop techniques that enable execution on current hardware. These techniques range from improved computational strategies (e.g., using multiple processors) to mathematical (e.g., the development and use of simplified surrogate models, perhaps constructed using advanced mathematical techniques such as line or subset sampling, artificial neural nets, or genetic algorithms [32]). From a reviewer’s perspective, many of these techniques are extremely complex, and their implementation will likely be difficult to explore in any depth; an input/output (“black box”) review approach might be the only practical approach available.
- Many ADPRA developers and even PRA analysts appear to believe that increased modeling detail automatically means more predictive accuracy. Although this seems

³¹ Note that the military acknowledges the difficulty in “validating” military simulations and refers to model verification, validation and accreditation (VV&A) to emphasize the importance of assuring that the model is acceptable for its intended use [52].

³² As an example relevant to Level 3 PRA, one traffic simulation model used to determine the acceptability of offsite emergency response plans addresses variations in average traffic speeds due to different weather conditions, but does not explicitly consider less likely but potentially system-disruptive events (e.g., traffic accidents, drivers disobeying directions and heading counter to the general traffic flow) [53].

³³ Note that in situations involving ADPRA, direct (also called “crude” or “brute force”) Monte Carlo sampling is unlikely to develop an adequate sample covering such events. Alternate approaches (e.g., dynamic event trees, importance sampling, subset sampling) are needed.

reasonable, there are practical situations where additional modeling detail can increase the likelihood of model error. Two examples are as follows.

- As discussed previously, a typical ADPRA model is composed of sub-models, many of which require input parameters whose uncertainties are represented by probability distributions that are supplied by the analyst. Poorly known parameters, by definition, should be represented by broad probability distributions. Depending on sub-model specifics, this can increase the likelihood that an ADPRA analysis will sample input values that are outside the range of applicability of the sub-model and lead to invalid results.³⁴
- The sub-models in an ADPRA model can be developed by different technical disciplines and might not be developed to the same degree of detail. Such modeling heterogeneities can lead to incongruous results. For example, in one early analysis that combined a highly simplified T-H model with an operating crew model, some situations gave rise to mismatches between the simplified T-H model predictions and the crew's operating procedures (which are based on more realistic models) [6].

Lessons from reviews of ADPRAs might suggest specific reviewer guidance regarding appropriate levels of modeling detail. In the meantime, my only suggestion is to be wary of assuming that detail ensures accuracy.

- Another potential pitfall arising from the ADPRA mindset is due to its focus on mechanistic modeling. This approach is philosophically the same as that underlying “reliability physics” (also called “physics-of-failure”) modeling approaches suggested for such applications as passive piping system reliability [54] and common-cause failure analysis [55], and is potentially advantageous because it explicitly introduces engineering knowledge (encoded through phenomenological models) into the PRA. The potential problem, of course, concerns model completeness. Unless the model covers all potentially important mechanisms, it will underestimate risk. Three examples, not necessarily dynamic but still relevant, are as follows.
 - At one plant, a worker broke a gas line and caused an explosion and subsequent fire when he stepped on to reach an object higher up. A generic load-resistance structural reliability model can, of course, treat this situation but the analyst must consider the possibility of such a load. (Also of course, the mechanistic model must include the gas line in the first place.)
 - At a different plant, operators tripped one unit when communications were lost with a diver who was in the common circulating water pump house, inspecting

³⁴ A similar situation can arise where the community state-of-knowledge regarding a parameter is actually reasonably good, but the analyst chooses to represent the state-of-knowledge using an overly broad distribution that discounts this knowledge.

condenser piping for the sister unit (which was shut down and defueled).³⁵ Again, such a scenario can be treated with a mechanistically-oriented analysis, but the possibility of the observed chain events needs to be recognized.³⁶

- The issue of rectifiability, i.e., the degree of credit for fixes of identified problems, has long been a point of contention in the PRA community [57]. It would appear that an increased focus on mechanistic modeling would increase the temptation to take complete credit for fixes of the mechanisms modeled.

Regarding the first two examples, a review of potentially relevant operational experience might be an effective way to identify at least some situations not covered by the ADPRA models. For the last example, it is still a matter of controversy as to how rectifiability should be treated by the PRA community, let alone ADPRA developers, users, and reviewers.

In general, I expect that details often matter for an ADPRA, perhaps even more than for classical PRAs, because of the potential for high complexity (and resulting non-linearities) in the ADPRA model that provide a key motivation for the ADPRA approach in the first place.³⁷ For a reviewer, it appears that the importance of details increases the importance of having a tool to explore the potential effects of changes in how these details are modeled, considered both singly and in meaningful groups.

4.3. Searching for Failures

In general, the NPP PRA community understands that the insights from a PRA (e.g., the principal scenarios, mechanisms, and factors contributing to risk) are at least as important as the “bottom line” results (in terms of CDF, large release frequency – LRF, etc.). Some ADPRA developers appear to be more bottom-line focused – in discussions of the advantages of ADPRA, they emphasize how their tools will result in better risk estimates, and spend little time discussing how the same tools will help develop improved insights. Perhaps improved insights are taken as a given.

More fundamentally, the ADPRA approach to modeling, consistent with broader applications of simulation modeling, is inductive – it assumes that by exercising the simulation model, important scenarios will be revealed. The challenge is, of course, that ultimate system risk might be significantly affected or even dominated by unlikely events and processes sampled rarely (or not at all), or even judged to be so unlikely as not to be included in the model.

³⁵ This event was captured in a review of Licensee Event Reports (LERs) involving multi-unit events [56].

³⁶ This is not to say that statistically-oriented common-cause failure models currently used in PRAs are “better” than proposed mechanistic models. However, they do have the advantage of including events that might not be explicitly recognized by mechanistic modelers. They also reduce possible temptations to dismiss complex scenarios that are difficult to treat with available tools.

³⁷ Note that despite its multiplicity of failure scenarios, a conventional PRA model (certainly a Level 1 model) is largely linear with respect to its inputs, and is mathematically quite well-behaved [58].

The ADPRA development community has at least partially recognized this challenge, and has also recognized that classical risk importance measures are insufficient (since some important drivers might be associated with continuous phenomena rather than failure events). Developers have addressed (or are addressing) this challenge directly through the use of global sensitivity analysis [59-61]³⁸ and indirectly through the use of advanced mathematical methods to create simplified, surrogate system models [32]. These methods, although sound in principle, appear to be computationally demanding. I don't know if they are ready for routine application, nor do I know if, at their current state of development, they produce insights readily usable by potential ADPRA reviewers.

In the absence of practically proven aids to search for important scenarios and mechanisms, I can only suggest that reviewers: a) continue to employ the same questioning attitude they would employ for any complex model,³⁹ and b) seek to obtain tools that will facilitate "what-if" explorations. (If the actual ADPRA is unavailable or too complicated to use, perhaps a simplified version, (e.g., a surrogate model similar to those created to facilitate uncertainty analyses, might suffice.)

4.4. Sensemaking

Because an ADPRA needs to consider both aleatory and epistemic uncertainties, as well as the system dynamics addressed by deterministic T-H codes for each sampled scenario, an ADPRA can generate enormous amounts of output. Making sense of this "Big Data" is a challenge recognized and being addressed by ADPRA developers (e.g., see [15]). For a reviewer, the challenge is to ensure that the sensemaking techniques are being appropriately applied, and are not: a) masking potentially useful insights, or b) implying an exaggerated sense of importance of other insights.

Regarding the concern about insight masking, techniques that aggregate dynamic scenarios based on user-defined factors might group low-likelihood/high-consequence scenarios with more likely but less-consequential scenarios if the factors are not defined to draw attention to the former. Similar to low frequency/high conditional core damage probability (CCDP) scenarios in conventional PRA, such scenarios could be of interest to reviewers, at least as a starting point for questions regarding the likelihood analysis.

Regarding the concern about potentially exaggerated importance, some methods of communicating key scenario elements (e.g., video animations of external flooding) can both convey an image of extreme precision and have a strong visceral impact. These subjective impressions can increase the apparent importance of the scenarios over that of scenario

³⁸ Borgonovo et al. address the issue of global sensitivity analysis for conventional PRA [62].

³⁹ As a particular dynamic example, if an analysis is taking credit for slowly developing processes that afford considerable time for crew actions, a natural question is if the process changes are too slow to trigger immediate action. Other, potentially dynamic examples could involve situations that reactor designers are trying to avoid, e.g., water in the core of a graphite-moderated high-temperature gas reactor, operating regimes with positive void coefficients in a sodium-cooled fast reactor.

elements (e.g., plant staff failing to re-align a system after testing) that don't lend themselves to such dramatic portrayals.

As with the preceding discussions regarding model data, V&V, and search aids, it seems useful for reviewers to have some type of review tool to probe beyond results and text-based model descriptions provided by an applicant.

5. Opinion and Potential Next Steps

At the risk of attempting to predict the behavior of a highly dynamic and non-linear system, I think that dynamic PRA in general, and ADPRA in particular, will become useful tools – perhaps even tools of choice – for PRA and RIDM. The broader PRA community's acceptance of these tools will likely take several years, but eventual change seems inevitable.

Although there are technical benefits to be gained from dynamic PRA (notably its potential to address such tough problems as passive systems T-H reliability and operator errors of commission, and its current ability to address simpler problems such as credit for FLEX), my reasons are largely non-technical.

- A. The simulation-oriented outlook of dynamic PRA is consistent with my understanding of current engineering trends (as supported by engineering education).
- B. Dynamic PRA is attractive to U.S. and international researchers and students, all of whom will eventually influence the future direction of PRA.
- C. Conversely, due to retirement and other causes, the PRA community is losing and will continue to lose many of the expert practitioners and advocates of conventional event tree/fault tree analysis.
- D. Tools for many forms of dynamic PRA are available (if not necessarily well-known in the broad PRA community), and many of the technical barriers to practical implementation of ADPRA are being addressed.

Another potential driver for increased use of dynamic PRA, albeit more indirect than the above points, is a general agency direction to make better, earlier use of diverse opinions. Such a direction would put greater value on serious explorations of model uncertainty and could lead to increased appreciation of the results and insights from non-traditional PRA analyses as complements to those from conventional analyses.⁴⁰

Of course, dynamic PRA is not the best tool for many PRA problems. There are many important PRA modeling challenges (e.g., the treatment of many types of common cause failures) that are not inherently dynamic, at least on the surface. Further, there are other situations where a

⁴⁰ Arguably, ensemble model predictions (as illustrated by hurricane path predictions) can be more valuable than a "best-estimate plus uncertainty" approach in some decision making applications. Indeed, non-traditional efforts to explore whether a range of predictions is sufficiently broad might be warranted.

classical analysis would likely be better (i.e., more efficient, and perhaps even more insightful).⁴¹ Nevertheless, I think a future trend towards the increased use of dynamic PRA is ongoing and that, as mentioned earlier, eventual acceptance by the broader PRA community is inevitable.

The current challenges to nearer-term adoption of dynamic PRA are not limited to technical issues. Economic and socio-organizational challenges are also important. Addressing these challenges will likely involve changes in the attitudes of different technical communities, and will probably not occur quickly (if at all) absent a new, strong driving force (e.g., a major industry initiative).

I recognize that in a practical regulatory support environment, resources for long-term R&D are always constrained. Nevertheless, I believe that positive activity will better place NRC for potential future applications. I therefore make the following recommendations for near-term activities.

1. Time and resources (e.g., for travel and conference/meeting participation) should be provided to enable selected NRC staff to catch up (and keep up) with developments. Staff activities include:
 - a. developing a better understanding of the voluminous and often complex dynamic PRA literature, particularly that related to insights from applications, but not neglecting mathematically-oriented methods documents (since the latter could be beneficial to broader uncertainty and sensitivity analysis activities relevant to RIDM); and
 - b. maintaining awareness of key domestic and international developments.
2. NRC/RES should serve as an active “cheerleader” for dynamic PRA. Beyond voicing support for advances,⁴² this could include such activities as:
 - a. identifying problems where existing tools could be useful and exercising these tools, thereby gaining/sharpening analysis skills as well as developing potentially useful insights;
 - b. offering to participate as a reviewer for selected ADPRA projects.
3. NRC/RES should participate (at least as a limited partner) on cooperative ADPRA projects. In addition to the activities above, this could mean active participation in (or perhaps even advocacy and leadership of) potential activities organized by the Nuclear Energy Agency’s Working Group on Risk Assessment (WGRISK) or by the International Atomic Energy Agency (IAEA).
4. NRC/RES should develop and implement a research plan for the longer-term development of advanced PRA methods, models, tools, and supporting data. (Note

⁴¹ As a crude analogy, comparing the performance of an operator skilled with the use of a slide rule and one skilled with Excel, the former can actually out-perform the latter in certain situations. (Consider the startup time for the latter, let alone non-routine situations involving a forced system update or a loss of power.) I might even speculate that the slide rule operator would not be enamored of the multiple significant digits produced by many computer-based analyses, and might actually have a better sense of the order of magnitude of results. Similarly, comparisons can be made between engineers who prefer to rely on qualitative understanding supported by “back-of-the-envelope” calculations and those who lean heavily on complex system codes.

⁴² Conversations with developers indicate that such expressions from NRC can indeed be useful to various stakeholders.

that such methods development activities would be consistent with past recommendations from the Advisory Committee on Reactor Safeguards – ACRS – in their reviews of the NRC’s PRA-related research activities.⁴³) The plan development process, which would presumably consider but not be limited to dynamic PRA,⁴⁴ would identify and prioritize activities based on normal considerations, e.g., anticipated regulatory needs (both near- and long-term), intended use of research products (practicality and value), technical feasibility of development, and costs. The plan itself would serve as a means for communicating planned activities and their basis.

Given the likely slow pace of dynamic PRA acceptance in the broader community, it might be questioned whether the staff should do anything now or wait until some future date. Given the relatively small resources involved in the above activities, I think any cost-savings from waiting are not worth the likely downsides (e.g., falling further behind an advancing field, not taking advantage of upcoming leverage opportunities, losing the opportunity to provide NRC perspectives regarding RIDM needs as the field progresses).

Acknowledgments

I gratefully acknowledge the assistance of V. Rychkov (EDF), E. Meléndez Asensio (CSN), C. Smith (INL), M. Denman (SNL), K. Coyne (NRC), J. Kanney (NRC), M. Gonzalez (NRC), and the NRC Technical Library staff in obtaining source material for this paper. I also thanks reviewers of an earlier draft for their comments.

⁴³ For example, NUREG-1635, Vol. 11 [63] expresses a concern that “[E]xtensions of PRA scope and the development of new methods have not been priorities.” NUREG-1635 Vol. 12 [64] recommends technology transfer activities that “will allow RES staff to focus more effectively on advancement of state-of-the-art risk assessment methods and practices.”

⁴⁴ For example, it could address such wide-ranging topics as Bayesian Belief Nets, improved qualitative methods to aid searches for failure scenarios, quantitative methods for multiple hazards, methods to address early life-cycle risks, improved “early warning” precursor-based indices, and “Big Data/artificial intelligence” applications.

References

Note: The literature on dynamic PRA is voluminous and the literature on simulation modeling potentially relevant to dynamic PRA is even more voluminous. The following list of references is representative but far from complete.

- [1] N. Siu, "Risk assessment for dynamic systems: an overview," *Reliability Engineering and System Safety*, **43**, 43-73, 1994.
- [2] A. Amendola and G. Reina, "Event sequences and consequence spectrum: a methodology for probabilistic transient analysis," *Nuclear Science and Engineering*, **77**, 297-315, 1981.
- [3] J.-M. Lanore, C. Villeroux-Lombard, F. Bouscatie, and A. Pavret de la Rochefordiere, "Probabilistic analysis of the loss of the decay heat removal function for Creys-Malville Reactor," *Proceedings International Conference on the Safety of Fast Liquid Metal Reactors*, Lyon, France, December 19-23, 1982.
- [4] A. Amendola and G. Reina, "DYLAM-1: A Software Package for Event Sequence and Consequences Spectrum Methodology," *EUR 9224 EN*, Commission of European Communities Joint Research Center (CEC-JRC), Ispra, Italy, 1984.
- [5] T. Aldemir, "Computer-assisted Markov failure modeling of process control systems," *IEEE Transactions on Reliability*, **R-36**, 133-44, 1987.
- [6] C. Acosta and N. Siu, "Dynamic event trees in accident sequence analysis: application to steam generator tube rupture," *Reliability Engineering and System Safety*, **41**, 135-154, 1993.
- [7] K.S. Hsueh and A. Mosleh, "The development and application of the accident dynamic simulator for dynamic probabilistic risk assessment of nuclear power plants," *Reliability Engineering and System Safety*, **52**, 297–314, 1996.
- [8] Y. Adolfsson, J.E. Holmberg, I. Karanta, and P. Kudinov, *Proceedings IDPSA-2012 – Integrated Deterministic-Probabilistic Safety Analysis Workshop*, Stockholm, Sweden, November 19-21, 2012. (Available from: <https://www.vtt.fi/inf/julkaisut/muut/2012/VTT-R-08589.pdf>)
- [9] J.-M. Izquierdo-Rocha and M. Sanchez-Perea, "Application of the integrated safety assessment methodology to the emergency procedures of a SGTR of a PWR," *Reliability Engineering and System Safety*, **45**, 159–173, 1994.
- [10] C. Smith, C. Rabiti, and R. Szilard, "Light Water Reactor Sustainability Program: Risk-Informed Safety Margins Characterization (RISMC) Pathway Technical Program Plan," *INL/EXT-17-43243, Rev. 0*, Idaho National Laboratory, Idaho Falls, ID, September 2017. (Available from: <http://www.inl.gov/lwrs>)
- [11] T. Aldemir, N. Siu, A. Mosleh, P.C. Cacciabue, and G. Goktepe, *Reliability and Safety Assessment of Dynamic Process Systems*, Springer-Verlag, 1994.
- [12] T. Aldemir, "A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants," *Annals of Nuclear Energy*, **52**, 113-124, 2013.
- [13] *Advanced Concepts in Nuclear Energy Risk Assessment and Management*, T. Aldemir, ed., World Scientific Publishing Co., 2018. (Available from: <https://www.worldscientific.com/worldscibooks/10.1142/10587>)

- [14] J. LaChance, J. Cardoni, Y. Li, A. Mosleh, D. Aird, D. Helton, and K. Coyne, “Discrete Dynamic Probabilistic Risk Assessment Model Development and Application,” SAND2012-9346, Sandia National Laboratories, Albuquerque, NM, October 2012. (ADAMS ML12305A351)
- [15] D. Mandelli, D. Maljovec, A. Alfonsi, C. Parisi, P. Talbot, J. Cogliati, C. Smith, and C. Rabiti, “Mining data in a dynamic PRA framework,” *Progress in Nuclear Energy*, **108**, 99-110, 2018.
- [16] Z. Jankovsky, M. Denman, and T. Aldemir, “Recent analysis and capability enhancements to the ADAPT dynamic event tree driver,” *Proceedings 14th International Conference on Probabilistic Safety Assessment and Management (PSAM 14)*, Los Angeles, CA, September 16-21, 2018.
- [17] Z. Jankovsky, T. Haskin, and M. Denman, “How to ADAPT,” SAND2018-6660, Sandia National Laboratories, June 2018.
- [18] Nuclear Energy Agency, “Use and Development of Probabilistic Safety Assessment: An Overview of the Situation at the End of 2017,” in publication.
- [19] U.S. Nuclear Regulatory Commission, “In the Matter of Docket Nos. 50-247-SP and 50-286-SP,” *Opinions and Decisions of the Nuclear Regulatory Commission with Selected Orders*, CLI-85-6, Vol. 21, Book II of II, May 1, 1985-June 30, 1985, pp. 1043-1103.
- [20] D.C. Bley, D.R. Buttemer, and J.W. Stetkar, “Light water reactor sequence timing: its significance to probabilistic safety assessment modeling,” *Reliability Engineering and System Safety*, **22**, 27-60, 1988.
- [21] S.D. Roberts and D. Pegden, “The history of simulation modelling,” *Proceedings of the 2017 Winter Simulation Conference*, W.K.V. Chan, A. D’Ambrogio, G. Zacharewitz, N. Mustafee, G. Wainer, and E. Page, eds., Las Vegas, NV, December 3-6, 2017.
- [22] D. Goldsman, R.E. Nance, and J.R. Wilson, “A brief history of simulation,” *Proceedings of the 2017 Winter Simulation Conference*, M.D. Rossetti, R.R. Hill, B. Johansson, A. Dunkin, and R.G. Ingalls, eds., Austin, TX, December 13-16, 2009.
- [23] N. Siu, K. Coyne, and N. Melly, “Fire PRA maturity and realism: a technical evaluation,” U.S. Nuclear Regulatory Commission, March 2017. (ADAMS ML17089A537)
- [24] N. Diaz, “Realism and conservatism,” *NRC Commissioner Speech S-03-023*, 2003 Nuclear Safety Research Conference, Washington, DC, October 20, 2003. (ADAMS ML032940250)
- [25] J. Corson, D. Helton, M. Tobin, A. Bone, M. Khatib-Rahbar, A. Krall, L. Kozak, and R. Buell, “Confirmatory Thermal-Hydraulic Analysis to Support Specific Success Criteria in the Standardized Plant Analysis Risk Models—Byron Unit 1,” *NUREG-2187*, January 2016.
- [26] C. Queral, J. Gómez-Magán, C. París, J. Rivas-Lewicky, M. Sánchez-Perea, J. Gil, J. Mula, E. Meléndez, J. Hortal, J.M. Izquierdo, and I. Fernández, “Dynamic event trees without success criteria for full spectrum LOCA sequences applying the integrated safety assessment (ISA) methodology,” *Reliability Engineering and System Safety*, **171**, 152-168, 2018.
- [27] C. París, C. Querala, J. Mula, J. Gómez-Magán, M. Sánchez-Perea, E. Meléndez, J. Gil, “Quantitative risk reduction by means of recovery strategies,” *Reliability Engineering and System Safety*, **182**, 13-32, 2019.

- [28] C. Smith, "Computational Risk Assessment," Plenary Lecture, *ANS International Topical Meeting on Probabilistic Safety Assessment (PSA 2017)*, Pittsburgh, PA, September 24-28, 2017.
- [29] S. Prescott, D. Mandelli, R. Sampath, C. Smith, and L. Lin, "3D Simulation of External Flooding Events for the RISMIC Pathway," *INL/EXT-15-36773*, Idaho National Laboratory, September, 2015.
- [30] N. Siu, I. Gifford, Z. Wang, M. Carr, and J. Kanney, "Qualitative PRA insights from operational events," *Proceedings 14th International Conference on Probabilistic Safety Assessment and Management (PSAM 14)*, Los Angeles, CA, September 16-21, 2018.
- [31] L.P. Pagani, G. Apostolakis, and P. Hejzlar, "The impact of uncertainties on the performance of passive systems," *Nuclear Technology*, **149**, 129-140, 2005.
- [32] E. Zio and N. Pedroni, "How to effectively compute the reliability of a thermal-hydraulic passive system," *Nuclear Engineering and Design*, **241**, 310-327, 2011.
- [33] N. Siu, "Dynamic accident sequence analysis in PRA: A comment on 'Human Reliability Analysis - Where Shouldst Thou Turn?'," *Reliability Engineering and System Safety*, **29**, No. 3, 359-364, 1990.
- [34] D. Dube, B. Albinson, R. Wolfgang, M. Saunders, and G. Krueger, "Exelon economic enterprise risk modelling of a BWR," *Proceedings ANS International Topical Meeting on Probabilistic Safety Assessment (PSA 2017)*, Pittsburgh, PA, September 24-28, 2017.
- [35] J. Devooght and C. Smidts, "Probabilistic reactor dynamics-I: The theory of continuous event trees," *Nuclear Science and Engineering*, **111**, 229-240, 1992.
- [36] J.T. Oden, T. Belytschko, J. Fish, T.J.R. Hughes, C. Johnson, D. Keyes, L. Petzold, D. Srolovitz, and S. Yip, *Revolutionizing Engineering Science through Simulation*, National Science Foundation Blue Ribbon Panel on Simulation-Based Engineering Science, May 2006.
- [37] U.S. Nuclear Regulatory Commission, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," *NUREG-1150*, December 1990.
- [38] U.S. Nuclear Regulatory Commission, "Loss of Main and Auxiliary Feedwater Event at the Davis-Besse Plant on June 9, 1985," *NUREG-1154*, July 1985.
- [39] National Research Council, *Modeling and Simulation: Linking Entertainment and Defense*, National Academy Press, Washington, D.C., 1997.
- [40] C.R. Wetteland, J.L. Miller, J. French, K. O'Brien, and D.J. Spooner, "The human simulation: resolving manning issues onboard DD21," *Proceedings 2000 Winter Simulation Conference*, J.A. Jones, R.R. Barton, K. Kang, and P.A. Fishwick, eds., Orlando, FL, December 10-13, 2000.
- [41] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*, McGraw-Hill, NY, 1965.
- [42] H. Charaibi, J.C. Houdebine, and A. Sibling, "PyCATSHOO: Toward a new platform dedicated to dynamic reliability assessment of hybrid systems," *Proceedings 13th International Conference on Probabilistic Safety Assessment and Management (PSAM 13)*, Seoul, Korea, October 2-7, 2016.

- [43] F. Aubert, B. Baude, P. Gauthé, M. Marquès, N. Pérot, F. Bertrand, C. Vaglio-Gaudard, V. Rychkov, and M. Balmain, "Implementation of probabilistic assessments to support the ASTRID decay heat removal systems design process," *Nuclear Engineering and Design*, **340**, 405-413, 2018.
- [44] Y.-H. Chang and A. Mosleh, "Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents. Part 1: Overview of the IDAC model," *Reliability Engineering and System Safety*, **92**, 997-1013, 2007.
- [45] K. Coyne and A. Mosleh, "Nuclear plant control room operator modeling within the ADS-IDAC, Version 2, dynamic PRA environment: Part 1 - General description and cognitive foundations," *International Journal of Performability Engineering*, **10**, 691-703, 2014.
- [46] M. Kloos and J. Peschke, "MC-DET: A probabilistic dynamics method combining Monte Carlo simulation with the discrete dynamic event tree approach," *Nuclear Science and Engineering*, **153**, 137-156, 2006.
- [47] A. Alfonsi, C. Rabiti, D. Mandelli, J. Cogliati, R. Kinoshita, and A. Naviglio, "RAVEN and Dynamic Probabilistic Risk Assessment: Software Review," *INL/CON-14-31785*, September 2014. (Available from: <https://inldigitallibrary.inl.gov/sites/sti/sti/6582263.pdf>)
- [48] U.S. Nuclear Regulatory Commission, "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," *WASH-1400 (NUREG-75/014)*, 1975.
- [49] H. Lewis, R.J. Budnitz, H.J.C. Kouts, W.B. Loewenstein, W.D. Rowe, F. von Hippel, and F. Zachariassen, "Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission," *NUREG/CR-0400*, 1978.
- [50] C. Picoco, V. Rychkov, and T. Aldemir, "Developing the control logic of thermal-hydraulic model for dynamic event tree generation with RAVEN-MAAP5-EDF," *Proceedings of ANS Best Estimate Plus Uncertainty International Conference (BEPU 2018)*, Real Collegio, Lucca, Italy, May 13-19, 2018.
- [51] K. Coyne and A. Mosleh, "Dynamic probabilistic risk assessment model validation and application – experience with ADS-IDAC, Version 2.0," in *Advanced Concepts in Nuclear Energy Risk Assessment and Management*, T. Aldemir, ed., 2018. World Scientific Publishing Co., 2018. (Available from: <https://www.worldscientific.com/worldscibooks/10.1142/10587>)
- [52] U.S. Department of Defense, "DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation," Instruction 5000.61, December 9, 2009, updated October 15, 2018. (Available from <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500061p.pdf>)
- [53] IEM, Inc., *Evacuation Time Estimates for the Vogtle Electric Generating Plant*, IEM/TEC12-1003, July 2013. (ADAMS ML13214A044)
- [54] C.L. Smith, V.N. Shah, T. Kao, and G. Apostolakis, *Incorporating Aging Effects into Probabilistic Risk Assessment – A Feasibility Study Utilizing Reliability Physics Models*, NUREG/CR-5632, August 2001.
- [55] Z. Mohaghegh, M. Modarres, and A. Christou, "Physics-based common cause failure modelling in probabilistic risk analysis: a mechanistic perspective," *Proceedings ASME Power Conference, Vol. 2*, Denver, CO, July 12-14, 2011.

- [56] S. Schroer and M. Modarres, "An event classification schema for evaluating site risk in a multi-unit nuclear power plant probabilistic risk assessment," *Reliability Engineering and System Safety*, **117**, 40-51, 2013.
- [57] G. Apostolakis, S. Kaplan, B.J. Garrick, and R.J. Duphily, "Data specialization for plant specific risk studies," *Nuclear Engineering and Design*, **56**, 321-329, 1980.
- [58] R.E. Barlow and F. Proschan, *Mathematical Theory of Reliability*, Wiley, NY, 1965.
- [59] A. Saltelli, et al., *Global Sensitivity Analysis: The Primer*, Wiley, Chichester, England, 2008.
- [60] D.R. Langewisch, Uncertainty and Sensitivity Analysis for Long-Running Computer Codes: A Critical Review, S.M. Thesis, Massachusetts Institute of Technology, February 2010. (Available from <https://dspace.mit.edu/handle/1721.1/58285>)
- [61] T. Sakurahara, T., "Global importance measure methodology for Integrated Probabilistic Risk Assessment, *Proceedings International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA 2017)*, Pittsburgh, PA, September 24-28, 2017.
- [62] E. Borgonovo, G. Apostolakis, S. Tarantola and A. Saltelli, "Comparison of global sensitivity analysis techniques and importance measures in PSA," *Reliability Engineering and System Safety*, **79**, 175-185, 2003.
- [63] Advisory Committee on Reactor Safeguards, "Review and Evaluation of the Nuclear Regulatory Commission Safety Research Program," *NUREG-1635, Vol. 11*, December 2014.
- [64] Advisory Committee on Reactor Safeguards, "Review and Evaluation of the Nuclear Regulatory Commission Safety Research Program," *NUREG-1635, Vol. 12*, April 2016.

Appendix A – Dynamic PRA FAQs

a) What is dynamic PRA?

Although there is no consensus definition of “dynamic PRA,” the PRA community typically uses the term to refer to approaches that simulate system behavior and accident scenario development over time.⁴⁵ The term is used to draw a contrast with conventional, “static” PRA which represents accident scenarios as collections of events (success and failures) and which treats time through criteria defining success/failure.

b) Does the treatment of scenario dynamics necessarily imply a complicated analysis?

No. The dynamic PRA R&D community has focused on complicated problems (e.g., operator errors of commission) that require the coupled treatment of diverse phenomena (e.g., thermal hydraulics, plant hardware actions, operator behavior), but simpler approaches (e.g., direct, object-oriented simulation) are available for simpler (but still dynamic) problems.

c) Are mature methods and tools available?

General purpose simulation modeling tools that are capable of dealing with many dynamic problems have long been available. NPP-PRA oriented toolboxes facilitating treatment of some more complicated problems are also available. Tools to support fully-coupled analyses requiring the use of T-H system codes (e.g., TRACE, MELCOR, MAAP) are available as R&D tools.

d) Is a dynamic PRA too detailed to be PRA? (This FAQ is often phrased as assertion: PRA was never meant to model scenarios at the level of detail addressed by dynamic PRAs.)

No. There is nothing in the usual Kaplan and Garrick “triplet” definition of risk [A2] that requires scenarios to be modeled in the same manner (including the level of detail) as currently followed in conventional NPP PRAs. It is worth noting that for fundamentally continuous systems, the notion of a “scenario” needs to be extended beyond the common, discrete interpretation.

e) Are there standards for dynamic PRA?

Not yet. However, note that the ASME/ANS PRA standard for non-light water reactors (issued for trial use) [A3] explicitly allows the use of approaches other than conventional event tree/fault tree methods, as long as such approaches meet the High Level

⁴⁵ Aldemir refers to “dynamic methods” that enable “more seamless consideration of the stochasticity in system behavior with the physical laws governing its evolution.” [A1]

Requirements and the Supporting Requirements of the standard. Also, as discussed by Arndt [A4], a variety of software quality standards and guidance documents relevant to quality assurance for analytical codes are available and are being used in various NRC programs intended to support the analysis, review, and auditing of reactor designs.

- f) Have dynamic PRA methods, models, and tools been validated?

Similar to conventional PRA methods, models, and tools, and for similar reasons, dynamic PRA methods, models, and tools have not been validated in the traditional sense. As the field progresses, some form of formal quality assurance program and regulatory acceptance process, analogous to what is used for T-H system codes, will likely be required. Note that the military, recognizing the difficulties in validating simulation models, adds the notion of accreditation to V&V. For example, the Department of Defense explicitly refers to Modeling and Simulation Verification, Validation, and Accreditation (VV&A), where accreditation is defined as “[t]he official certification that a model or simulation and its associated data are acceptable for use for a specific purpose” [A5]. Note also that the dynamic PRA community is certainly aware of the concern, and is making progress. (See, for example, Coyne and Mosleh [A6, A7], Aubert et al. [A8], and Picoco et al. [A9].)

- g) Where are the major dynamic PRA development programs?

In the U.S., the centers of dynamic PRA development for NPPs are universities (particularly OSU, UCLA, and UMD, with the recent addition of University of Illinois Urbana-Champaign – UIUC) and national laboratories (particularly INL and SNL). In Europe, notable activities are being performed and/or supported by regulators with ties to universities (notably CSN, which is working with UPM), technical support organizations (notably GRS), and industry organizations (notably EDF and the Nordic PSA Group). Italy’s Politecnico di Milano has a long history of developing mathematical methods intended to support the performance of dynamic PRA and is also involved in IDPSA activities. Dynamic PRA is also a subject of growing interest in Korea (the Korea Atomic Energy Research Institute – KAERI, and a number of associated universities) and Japan (e.g., the University of Tokyo).

- h) What are the currently favored techniques for dynamic PRA?

Most dynamic PRA researchers are focusing on dynamic event trees (i.e., event trees that evolve over time). Work is also continuing on developing object-oriented simulation tools that are based on direct simulation techniques. Outside of the NPP arena, developers and analysts appear to favor direct simulation.

- i) Are there any reasons not to use dynamic PRA tools for simple situations?

In principle, even if it's overkill, a dynamic PRA model that uses the same fundamental modeling assumptions as a conventional PRA model should produce comparable results. Of course, if further modeling details are added to better represent the modeled system, this can introduce sensitivities in the results that might take additional effort to understand. Note also that if the analysis requires the treatment of rare events, the user should ensure that the dynamic PRA tool adequately addresses such events. This caution applies especially to dynamic PRA tools that rely on direct simulation, but dynamic event tree branching rules might also need scrutiny.

- j) Can a dynamic PRA analyze scenarios with events and conditions before the actual initiating event (where the initiating event is as defined as an event perturbing plant operation [A10])?

In principle, yes. Of course, in principle, conventional PRA models can also be applied for pre-initiating event scenario development. Current fire PRA models, which address possible events (fire ignition, growth, and suppression) preceding potential initiating events, provide one example. Also of course, the analysis, whether conventional or dynamic, needs appropriate sub-models for events preceding the initiating event.

References

- [A1] *Advanced Concepts in Nuclear Energy Risk Assessment and Management*, T. Aldemir (Ed.), World Scientific Publishing Co (2018). (Available from: <https://www.worldscientific.com/worldscibooks/10.1142/10587>)
- [A2] S. Kaplan, and B.J. Garrick, "On the quantitative definition of risk," *Risk Analysis*, **1**, 11–37, 1981.
- [A3] American Society for Mechanical Engineers and American Nuclear Society, Probabilistic Risk Assessment Standard for Advanced Non-LWR Nuclear Power Plants, ASME/ANS RA-S-1.4-2013, December 2013.
- [A4] S.A. Arndt, "Software quality assurance for analytical codes," *Transactions 2006 ANS Annual Meeting*, Reno, NV, June 4-8, 2006.
- [A5] U.S. Department of Defense, "DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation," Instruction 5000.61, December 9, 2009, updated October 15, 2018. (Available from <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500061p.pdf>)
- [A6] K. Coyne and A. Mosleh, "Dynamic probabilistic risk assessment model calibration and validation using simulator data - another application of HRA Empirical Study data," *Proceedings of PSAM 10, Tenth International Conference of Probabilistic Safety Assessment and Management*, Seattle, WA, June 14-19, 2010.

- [A7] K. Coyne and A. Mosleh, "Dynamic probabilistic risk assessment model validation and application – experience with ADS-IDAC, Version 2.0," in *Advanced Concepts in Nuclear Energy Risk Assessment and Management*, T. Aldemir, ed., 2018. World Scientific Publishing Co., 2018. (Available from: <https://www.worldscientific.com/worldscibooks/10.1142/10587>)
- [A8] F. Aubert, B. Baude, P. Gauthé, M. Marquès, N. Pérot, F. Bertrand, C. Vaglio-Gaudard, V. Rychkov, and M. Balmain, "Implementation of probabilistic assessments to support the ASTRID decay heat removal systems design process," *Nuclear Engineering and Design*, **340**, 405-413, 2018.
- [A9] C. Picoco, V. Rychkov, and T. Aldemir, "Developing the control logic of thermal-hydraulic model for dynamic event tree generation with RAVEN-MAAP5-EDF," *Proceedings of ANS Best Estimate Plus Uncertainty International Conference (BEPU 2018)*, Real Collegio, Lucca, Italy, May 13-19, 2018.
- [A10] M. Drouin, M. Gonzalez, S. Herrick, J.S. Hyslop, D. Stroup, J. Lehner, T. Pratt, M. Dennis, J. LaChance, and T. Wheeler, *Glossary of Risk-Related Terms in Support of Risk-Informed Decisionmaking*, NUREG-2122, November 2013.

Appendix B – Recovery Modeling: A Potential Application of Dynamic PRA

The modeling of recovery actions plays an important role in realistic PRA. These actions can be included in event trees or fault trees. As an example, Figure B.1, which is a slightly simplified event tree for a weather-related LOOP event at an isolation-condenser boiling water reactor (BWR), includes recovery actions for offsite power and for the emergency diesel generators (EDGs).

A typical PRA analysis will use an aleatory distribution for the time required to perform the recovery action (generated using empirical data and/or expert judgment) and a point estimate of the time available to generate the probability of recovery failure per the following equation:

$$P\{\text{failure to recover}\} = P\{T_R > T_A\} = \int_{T_A}^{\infty} f_{T_R}(t) dt \quad (\text{B.1})$$

where T_R is the time required, T_A is the time available, and $f_{T_R}(\cdot)$ is the probability density function for T_R . Eq. (B.1) is the complementary cumulative distribution function of T_R evaluated at T_A and can be easily determined (either analytically or from tables) for several distributional forms (e.g., Weibull, lognormal). For other forms, standard numerical solution schemes (e.g., trapezoidal rule, Simpson's rule, more advanced quadrature methods, or Monte Carlo integration) can provide more than sufficient accuracy for the purposes of a PRA.

In a more general case, T_A can be an aleatory variable. In such a case,

$$P\{T_R > T_A\} = \int_0^{\infty} \int_0^s f_{T_R, T_A}(s, t) dt ds \quad (\text{B.2})$$

where $f_{T_R, T_A}(\cdot, \cdot)$ is the joint density function of T_R and T_A . If T_R and T_A are independent,

$$P\{T_R > T_A\} = \int_0^{\infty} f_{T_R}(s) \left[\int_0^s f_{T_A}(t) dt \right] ds \quad (\text{B.3})$$

where the bracketed term is the cumulative distribution function for T_A . Standard numerical solution schemes can be used to solve Eqs. (B.2) and (B.3).

Eqs. (B.1) through (B.3) deal with a single recovery action. As can be seen in Figure B.1, a scenario can involve multiple recovery actions. More generally it can involve multiple actions, mitigation-related as well as recovery. Each action can have some effect on the plant, and the change in the plant behavior, in turn, provides an altered context for action. For example, following a LOOP, early crew actions to:

- a) extend the operation of the Emergency Core Cooling System (ECCS) by: i) ensuring a long-term supply of water for the isolation condenser, and ii) operating the isolation condenser manually when batteries are depleted; and
- b) shed non-critical DC loads to extend battery lifetimes

can increase the amount of time available to perform recovery actions. These dynamic interactions are modeled through the different time windows shown in Figure B.1. Of course, the

use of only four time windows is an approximation. A more detailed model could account for the effect of variations in such continuous variables as the amount of water in the Condensate Storage Tank (CST) and the timing of DC load shedding. Perhaps more importantly, a more detailed treatment of task performance could also account for dependencies across the different actions (e.g., due to limited staff resources) and for the likely parallel nature of some of the activities. Such a treatment could lead to different risk insights as well as more refined risk estimates.

Figure B.2 shows an event sequence diagram for a simulation-based dynamic model of power recovery for a plant with two EDGs [B1]. The model treats: a) time-dependent phenomena (battery drainage) as well as random runtime failures, and b) the parallel nature of offsite power and EDG recovery. The model also recognizes that battery drainage doesn't start until the associated EDG fails. For the plant analyzed, the number of available staff was judged sufficient to allow parallel recovery activities, but the model is capable of addressing dependencies due to resource limitations. (Note that such dependencies figured prominently in the Fukushima Dai-ichi reactor accidents.) It is worth noting that the model, which was constructed using SIMSCRIPT II.5 (a discrete event simulation language¹), was developed by an engineer knowledgeable of the plant's electrical distribution system and associated operations, but with little prior simulation modeling experience, and that the effort was relatively straightforward.

A second, and more involved dynamic analysis of recovery is provided by Paris et al. [B3]. This analysis uses the SCAIS methodology [B4] to treat the use of FLEX strategies in response to a loss of feedwater (LOFW) event at a PWR. This analysis treats dynamics introduced by plant thermal hydraulic behavior and thereby accounts for potential variations in the time available for operator action. Despite its simplified treatment of operator actions,² the model appears to provide a useful approach for evaluating FLEX implementations.

References

- [B1] T. J. McIntyre and N. Siu, "Electric power recovery at TMI-1: a simulation model," *Proceedings International ANS/ENS Topical Meeting on Thermal Reactor Safety*, San Diego, California, February 2-6, 1986, pp. VIII.6-1 through VIII.6-7.
- [B2] V.N. Dang, D.L. Deoss, and N. Siu, "Event simulation for availability analysis of dynamic systems," *Transactions Eleventh International Meeting on Structural Mechanics in Reactor Technology (SMiRT 11)*, Tokyo, Japan, August 18-23, 1991, **Vol. M**, pp. 31-36.
- [B3] C. París, C. Querala, J. Mula, J. Gómez-Magán, M. Sánchez-Perea, E. Meléndez, J. Gil, "Quantitative risk reduction by means of recovery strategies," *Reliability Engineering and System Safety*, **182**, 13-32, 2019.

¹ See Dang et al. [B2] for discussion on discrete event simulation in the context of systems availability analysis.

² In particular, the model uses fixed distributions for the timing of actions that: a) don't depend on the scenario evolution, and b) don't explicitly model cognitive behaviors that provide a rationale for decisions (e.g., to perform feed and bleed cooling). Such issues can be addressed by more complete (and complex) dynamic PRA platforms as ADS/IDAC [B5-B7].

- [B4] C. Queral, J. Gómez-Magán , C. París, J. Rivas-Lewicky, M. Sánchez-Perea, J. Gil, J. Mula, E. Meléndez, J. Hortal, J.M. Izquierdo, and I. Fernández, “Dynamic event trees without success criteria for full spectrum LOCA sequences applying the integrated safety assessment (ISA) methodology,” *Reliability Engineering and System Safety*, **171**, 152-168, 2018.
- [B5] K.S. Hsueh and A. Mosleh, “The development and application of the accident dynamic simulator for dynamic probabilistic risk assessment of nuclear power plants,” *Reliability Engineering and System Safety*, **52**, 297–314, 1996.
- [B6] Y.-H. Chang and A. Mosleh, “Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents. Part 1: Overview of the IDAC model,” *Reliability Engineering and System Safety*, **92**, 997-1013, 2007.
- [B7] K. Coyne and A. Mosleh, “Nuclear plant control room operator modeling within the ADS-IDAC, Version 2, dynamic PRA environment: Part 1 - General description and cognitive foundations,” *International Journal of Performability Engineering*, **10**, 691-703, 2014.

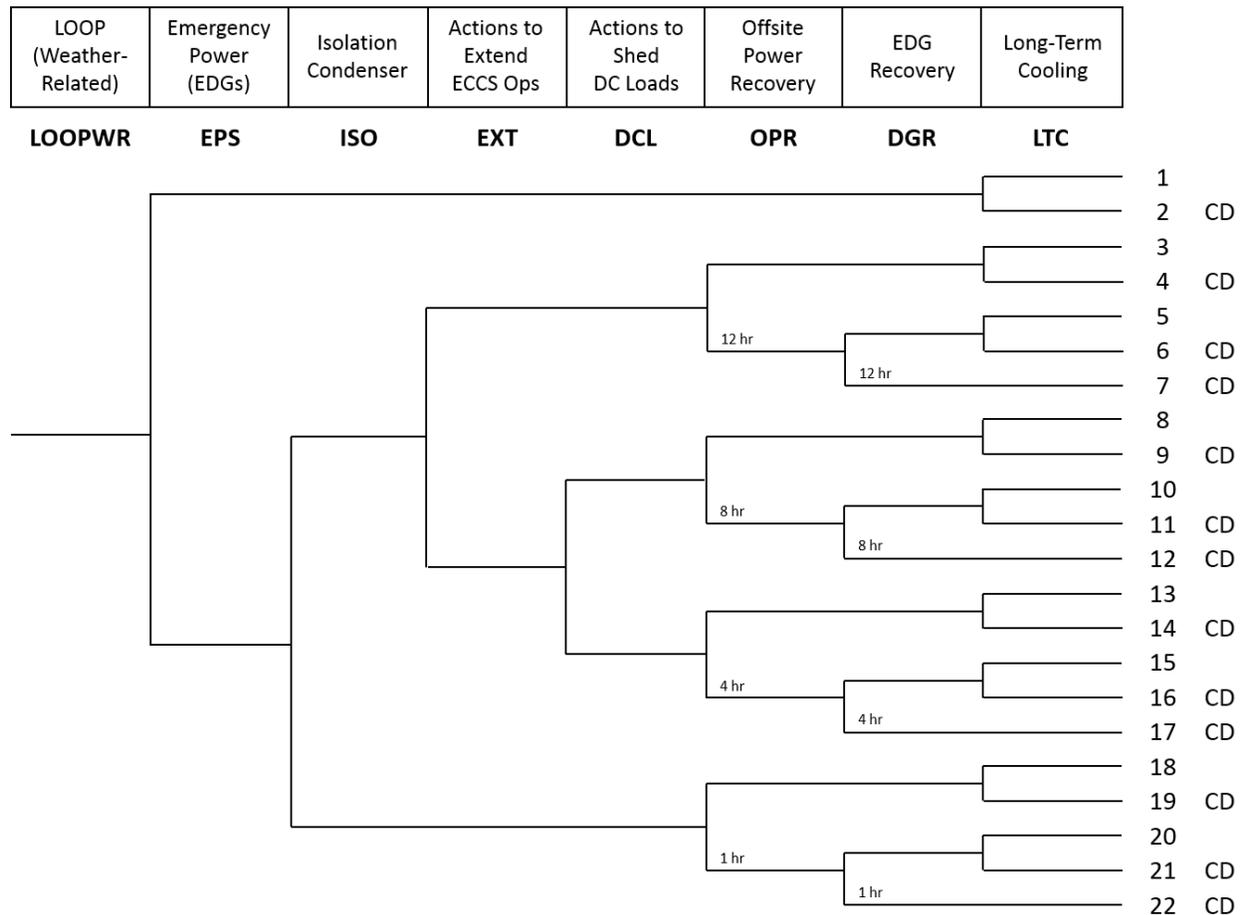


Figure B.1. Simplified Event Tree for LOOP at an Isolation Condenser BWR

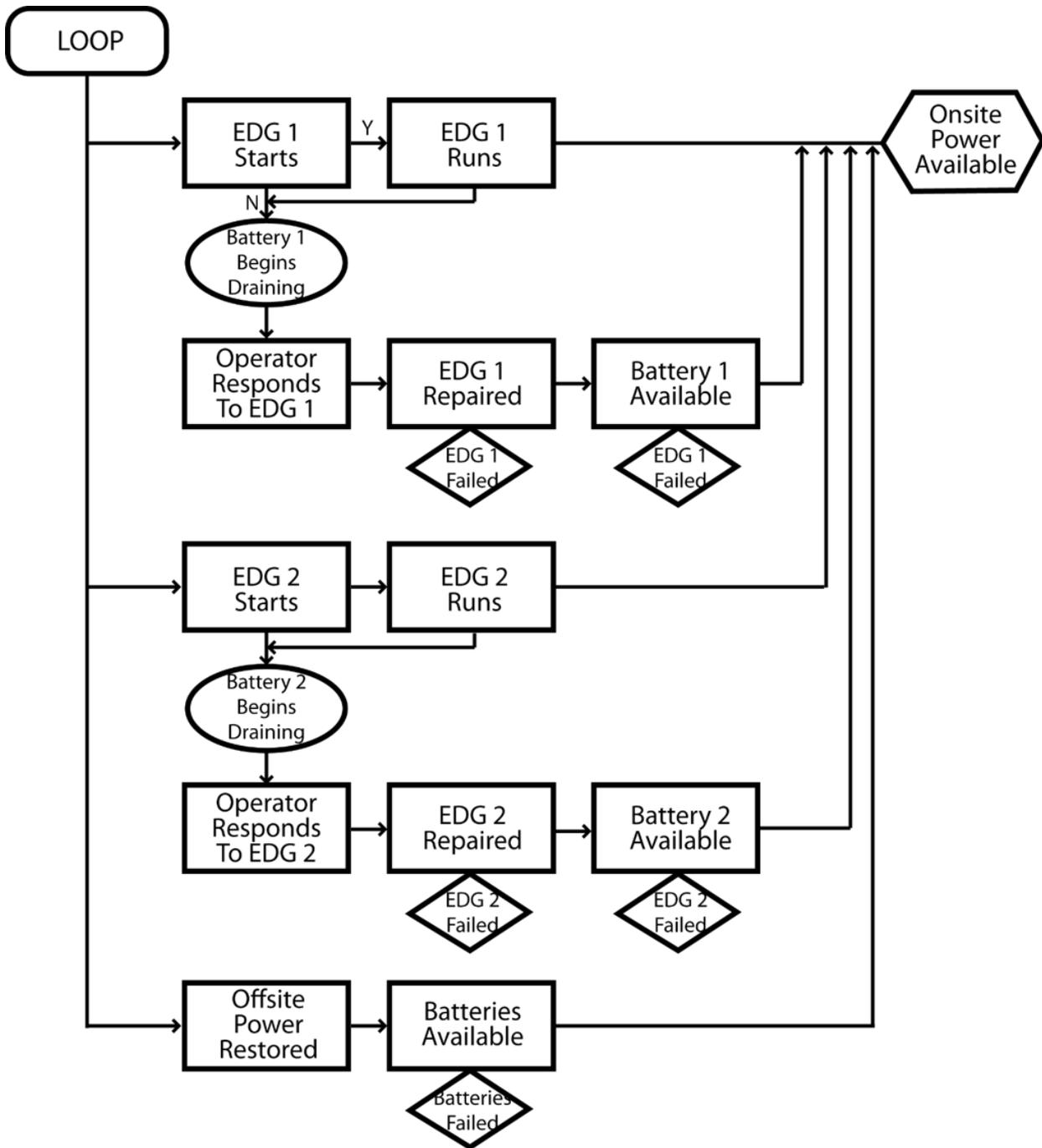


Figure B.2. Event Sequence Diagram for a Power Recovery Simulation Model [B1]

Appendix C – A Potential Application of a Simple Dynamic PRA

In 2018, a small project team performed review of a small number of operational events with the aim of identifying lessons useful for PRA model developers [C1]. The team identified an activity where a simple, yet still dynamic PRA analysis could be helpful for risk-informed decision making: plant preparations in advance of a storm. Two specific examples were identified.

The first example involved two international plants. In both cases, the plants lost offsite power due to high winds, prior to storm-induced flooding. In one case, it appears that the plant lost offsite power well before flooding, and it further appears that plant shutdown was relatively uncomplicated. In the second case, it appears that LOOP and the start of site flooding were roughly coincident, and the event required the mobilization of national resources in response. Recognizing that the plants are of very different designs (one plant was a gas reactor and the other a pressurized water reactor), nevertheless it can be reasonably hypothesized that the differences in the timing of hazard arrivals significantly affected the severity of the challenge to plant operations.

The Turkey Point/Hurricane Andrew incident provides another example of the importance of event timing. In this incident, the hurricane arrived two hours earlier than initially expected, with high winds (exceeding 48 km/h – 30 mph) starting roughly one hour after Unit 3 achieved Mode 4 but one hour before Unit 4 achieved Mode 4. It can be hypothesized that if the plant staff had not started their storm preparations as early as they did, plant shutdown operations, some of which involved outdoor actions, could have been significantly more challenging.

Nuclear power plants have, of course, procedures for responding to severe storm warnings. However, I do not know the extent to which contingencies built into these procedures are informed by considerations of potentially impactful time-dependent possibilities (e.g., changes in storm behavior, additional random or storm-induced failures of key functions that might preclude some shutdown options). It might be argued that such possibilities need not be identified and addressed if a plant takes a conservative approach biased toward early, precautionary shutdowns. However, such an approach, although desirable from a plant-centric point of view, might actually be undesirable from a regional emergency response point of view. It appears that dynamic PRA might be a useful tool for identifying risk-significant possibilities and suggesting risk-informed refinements to existing plant procedures.¹

It should be noted that the dynamic analysis might not need to be very complicated from a phenomenological point of view. It is conceivable that a fairly high-level task analysis approach,

¹ Note that operational choices made during at least two of the reviewed incidents considered potential future failures as well as the current plant conditions. However, it appears that at least in one case, these choices were made as the incident evolved, and did not benefit from detailed, systematic analyses prior to the incident.

Note also that at least some U.S. plants account for weather contingencies in their maintenance planning. However, this planning appears to be performed from a long-term point of view (e.g., considering whether a particular maintenance activity should be performed, given the possibility of severe weather during a particular season in the coming year), rather than at a more immediate, storm response level.

e.g., as exemplified by the approach used by Wetteland in a warship manning analysis [C2], could provide useful results. Such an analysis would need to address such factors as the time and resources required to perform various tasks and the sequencing of these tasks, but not necessarily more complicated considerations (e.g., decision maker cognition). The analysis would need to consider practical complexities (e.g., the staging of activities at multi-unit sites, economic as well as public-health consequences, offsite emergency response resources and needs, the possibility of unexpected developments and events) faced by actual decision makers, but these complexities also appear to be addressable within the framework of a task analysis approach.

References

- [C1] N. Siu, I. Gifford, Z. Wang, M. Carr, and J. Kanney, "Qualitative PRA insights from operational events," *Proceedings 14th International Conference on Probabilistic Safety Assessment and Management (PSAM 14)*, Los Angeles, CA, September 16-21, 2018.
- [C2] C.R. Wetteland, et al., "The human simulation: resolving manning issues onboard DD21," *Proceedings 2000 Winter Simulation Conference*, J.A. Jones, R.R. Barton, K. Kang, and P.A. Fishwick, eds., Orlando, FL, December 10-13, 2000.

Appendix D – On Technical Maturity

In 1981, Prof. C. Allin Cornell, a pioneer in the area of probabilistic seismic engineering and safety, wrote a paper on how one can assess the technical maturity of a field [D1]. The following table, developed for a discussion on fire PRA maturity and realism [D2], presents his concepts in tabular form.

Table D1. Indicators of stages of technical maturity (Siu et al., [D2], adapted from Cornell [D1])

	Developmental Stage		
	Early (Infancy, Emerging)	Intermediate (Adolescent, Developing)	Late (Mature, Stable)
Practitioners	<ul style="list-style-type: none"> • Small research community • Small number of practitioners • Strong personality influences, competing schools of thought 	<ul style="list-style-type: none"> • Larger number of practitioners • Larger number of experienced researchers 	<ul style="list-style-type: none"> • Many well-trained and experienced practitioners • Recognize limits of applicability of methods • Can adapt methods to new situations • Can work with researchers to identify important issues
Research Agenda	<ul style="list-style-type: none"> • Driven by perceived needs • Problem selection affected by personal choice (e.g., due to ease of formulation or solution) 	<ul style="list-style-type: none"> • New practice-driven research problems • Some consensus positions for some broadly defined problem areas • Some unproductive research lines abandoned • Incomplete coverage of topics 	<ul style="list-style-type: none"> • Most research driven by needs of practice • More abstract research addresses needs clearly identifiable by all concerned
Applications	<ul style="list-style-type: none"> • Local applications (addressing small parts of larger problems) • No broader framework 	<ul style="list-style-type: none"> • Fast growth • Developing vocabulary • Optimistic views on new methods; limitations not well understood 	<ul style="list-style-type: none"> • Vocabulary has evolved • General framework exists • Little “selling” of area

References

[D1] C.A. Cornell, “Structural safety: some historical evidence that it is a healthy adolescent,” *Proceedings Third International Conference on Structural Safety and Reliability (ICOSSAR '81)*, Trondheim, Norway, June 23-25, 1981.

[D2] N. Siu, K. Coyne, and N. Melly, “Fire PRA maturity and realism: a technical evaluation,” U.S. Nuclear Regulatory Commission, March 2017. (ADAMS ML17089A537)

Appendix E – Acronyms and Abbreviations

1-D	one-dimensional
3-D	three-dimensional
ADAMS	Agencywide Documents Access and Management System
ADAPT	software tool for dynamic PRA (not defined as an acronym)
ADPRA	advanced dynamic PRA
ADS/IDAC	Accident Dynamic Simulator/Information Decision Action Crew
ASP	accident sequence precursor
BWR	boiling water reactor
CCDP	conditional core damage probability
CDF	core damage frequency
CNRA	Committee of Nuclear Regulatory Authorities (OECD/NEA)
CSN	Consejo de Seguridad Nuclear (Spain)
CSNI	Committee for the Safety of Nuclear Installations (OECD/NEA)
DOE	U.S. Department of Energy
EDF	Electricité de France
ERM	enterprise risk management
ESRA	European Safety and Reliability Association
ESREL	European Safety and Reliability (conference series)
EU	European Union
FLEX	diverse and flexible mitigation strategies
GRS	Gesellschaft für Anlagen und Reaktorsicherheit (Germany)
HEAF	high energy arcing fault
HRA	human reliability analysis
HTGR	high-temperature gas reactor
IAEA	International Atomic Energy Agency
IAPSAM	International Association for Probabilistic Safety Assessment and Management
IDPSA	Integrated Deterministic-Probabilistic PSA
INL	Idaho National Laboratory
ISA	Integrated Safety Assessment
LER	Licensee Event Report
LOOP	loss of offsite power
LPSD	low power and shutdown
LRF	large release frequency
LWRS	Light Water Reactor Sustainability Program (DOE)
MIT	Massachusetts Institute of Technology
NEA	Nuclear Energy Agency (OECD)
NPP	nuclear power plant
NPSAG	Nordic PSA Group
NRC	U.S. Nuclear Regulatory Commission
OECD	Organization for Economic Cooperation and Development
OSU	Ohio State University

PRA	probabilistic risk assessment
PSA	probabilistic safety assessment
PSAM	Probabilistic Safety Assessment and Management (conference series)
PWR	pressurized water reactor
R&D	research and development
RAVEN	Risk Analysis Virtual Environment
RES	Office Nuclear Regulatory Research (NRC)
RIDM	risk-informed decision making
RISMC	Risk-Informed Safety Margin Characterization pathway (DOE)
SCAIS	Simulation Codes System for ISA
SNL	Sandia National Laboratories
SPAR	standardized plant analysis risk
T-H	thermal-hydraulic (also referred to as thermo-hydraulic)
UCLA	University of California at Los Angeles
UIUC	University of Illinois, Urbana-Champaign
UPM	Universidad Politécnica de Madrid
V&V	verification and validation
VV&A	verification, validation, and accreditation
WGRISK	Working Group on Risk Assessment (OECD/NEA/CSNI)
WSC	Winter Simulation Conference