Proceedings
of the
International Topical Meeting
on

Safety Margins in Criticality Safety

San Francisco, California
November 26-30, 1989

Sponsored by the American Nuclear Society's
Nuclear Criticality Safety Division

Published by the
American Nuclear Society, Inc.
La Grange Park, Illinois, 60525 USA

APPLICATIONS OF PRA TO CRITICALITY SAFETY AT ICPP

James R. Wilson
Westinghouse Idaho Nuclear Co., Inc.
P.O. Box 4000 (MS 3210)
Idaho Falls, Idaho 83403
(208) 526-1690

ABSTRACT
This paper presents historical and current applications of PRA to criticality safety. Currently, PRA (i.e., a probabilistic approach) is used alongside deterministic safety analysis as two separate legs of the approval process. However, PRA techniques are also used to optimize deterministic analysis (e.g., to validate independence or perform tradeoffs). A sample problem is presented to show how PRA is used in criticality safety.

First, I would like to present the historical perspective of the growing responsibilities of PRA at the ICPP. Then, I'd like to discuss the present status of PRA at the ICPP and some of the areas being developed further for criticality safety analysis. I will close with a simple illustration of the use of PRA in criticality safety.

HISTORICAL PERSPECTIVE

1980 -- Fault trees were used to determine where Technical Specifications/Standards (TS/Ss) should be applied and to assure their adequacy. Common cause failure and dependencies between human actions were not covered in depth.
1982 -- PRA was used to determine calibration/maintenance intervals and practices to reduce contributions from these sources.
1982 -- Probabilistic analysis was used in a specification dispute. The vendor found it too difficult to construct a PPS using passive cooling techniques and requested the use of active cooling with instrumentation to detect failure. The analysis demonstrated comparable reliability.
1983 -- PRA warned of the high failure probability for redundant PPS valves in series. This was later confirmed by failure reports (UORs) within the plant.
1984 -- PRA was used to evaluate the competing safety concerns of contamination control and criticality safety.
1984 -- An attempt was made to use PRA to prove a system was "safe enough". This could not be done because no quantitative criteria was established at the time. However, as a fallback, the fault tree was used to show barriers which, with adequate reinforcement, could be used in place of an expensive design upgrade.
1985 -- The first use of PRA in an ongoing accident investigation (noncriticality related).
1985 -- PRA was used to "validate" a PPS system without use of a quantitative cutoff criteria. The main contributors were reduced by design fixes and administrative controls until the analysis was "down in the grass" (i.e., any remaining fixes would have to address many scenarios).
1985 -- Quantitative criteria were established for PRAs by joint contractor/DOE discussions ($\leq 10^{-5}$/scenario-year and $\leq 10^{-4}$/facility-year). This only applied to new facilities. No criteria has yet been established for existing facilities, or for backfitting and upgrade.
1987-ongoing -- Detailed consequence calculation combined with fire and criticality scenarios in the same fault trees to allow tradeoffs between fire and criticality safety.

The purpose of this historical presentation is not to indicate that this sequence is the natural or best, but to show how we solved our problems in hope that others may find something of use in solving their problems.

CURRENT STATUS

At the ICPP, the double/triple contingency approach is used on upgrade projects, and double/triple contingency plus PRA are used on new construction.

For example, for a new facility, two independent and unlikely barriers must fail simultaneously before any shielded criticality

may occur. For any unshielded criticality, three such barriers must fail. In addition to this, a PRA is conducted to show adequate safety, necessary TS/Ss, and design tradeoffs.

However, the contingency approach itself can be challenging to apply. For instance, a "physical" barrier is one which depends upon actual equipment in the plant. An "administrative" barrier is one which depends upon correct operator/supervisor actions (e.g., a TS/S). And we know that a physical barrier is stronger than an administrative barrier. In addition, we've promised our DOE customer that in no case will plant safety depend upon two administrative barriers for a shielded criticality. Yet, how are barriers in between physical and administrative to be judged (e.g., sampling)? And, given a choice of barriers, how is the best chosen, economic concerns aside?

PRA is a valuable tool for judging overall barrier quality and if barriers are truly independent. Therefore, we have a synergistic approach where a new-project safety analysis must separately satisfy the contingency and the PRA criteria, yet the contingency analysis may be tweaked (i.e., have feedback) from the PRA study.

This PRA "tweaking" may be both in qualitative and quantitative senses.

QUALITATIVE ENHANCEMENT OF CONTINGENCIES

Three problems which occur in the contingency approach can be handled with simply a qualitative (no numbers calculated) fault tree: Missing scenarios, confused scenarios, and missed dependencies.

A mere listing of scenarios often misses key ones. Obviously, without a complete list of scenarios, the list of contingencies is inadequate. A properly constructed fault tree will strive for completeness on each level, thus greatly reducing the chances of missing scenarios.

In one contingency analysis at the ICPP, three contingencies were proposed for a shielded criticality scenario. Since only two contingencies were required, this presented the appearance of extra safety. Upon doing a fault tree, I discovered two independent scenarios within the "confused" scenario, one of the scenarios having only one contingency.

Contingencies, by definition, must be independent. In one scenario, contingencies may be independent, while in another, dependent. Indepth PRA analysis of contingencies can reveal these hidden dependencies. Thus, the discipline of the fault tree is the best way to discover all credible scenarios and hidden dependencies.

QUANTITATIVE ENHANCEMENT OF CONTINGENCIES

Contingencies must be "unlikely". This is defined at the ICPP as having a frequency of occurrence of once in 10 to 1000 years. The occurrence frequency is often difficult to determine without some type of PRA analysis. For example, one criticality contingency (a surveillance requirement) was not working as well as had been expected. At first, the operators and the shift supervision were blamed. However, on the basis of a PRA-type analysis, it was determined that they were doing well (8×10^{-5} and 2×10^{-3} per surveillance, respectively). The outcome was that such high-frequency human-based surveillance did not meet the "unlikely" criteria for a contingency, occurring at a calculated frequency of 7 times in 10 years, and some type of computer surveillance was recommended.

The probability of simultaneous failure of contingencies must also be unlikely. There is no better way to determine this than PRA.

Contingencies are not needed for "incredible" events. PRA can be used to "document" incredibility (individual events which do not qualify separately as contingencies can combine to make an incredible scenario). In one analysis, 18 separate failures fed an AND gate. Even if very conservative failure probabilities were assigned to each event, it was clear that a "nonscenario" was involved here.

For anyone who questions the value of PRA, try to do a design tradeoff analysis using contingencies. Barriers may soften or harden with the various design options, but how can you rank the designs, without some quantitative analysis?

AREAS OF CONCERN WITH PRA: COST

PRAs can be expensive, but much of this expense can be avoided with the following rule: There is no point in quantifying a fault tree (i.e., doing a PRA), without agreement on "how safe is safe

enough". One of the following criterion should be adopted prior to quantifying the fault trees:

1. Put additional barriers on high probability scenarios until you run out of money or all the scenarios are at about the same probability,

2. Do design tradeoffs, selecting the most cost effective safety improvements,

3. Design to a safety goal.

Most of the power of PRAs was unavailable to us until 1985, when our DOE customer met with us to establish quantitative safety goals. At first, they suggested a safety goal of 10^{-6}/year for a new facility. We felt such a goal would defeat the purpose of the PRA, forcing the analyst to "manipulate" the PRA, using unreasonable assumptions, to achieve the requisite probability frequency. After discussion, 10^{-4}/year was chosen.

A possible goal of 10^{-3}/year was also discussed, but DOE felt the facility designers should have a more difficult goal to meet, with the understanding that when we have problems meeting criteria, we would evaluate options and arrive at the best solution. Two important points are brought out by this:

1). The safety goal should be reasonable, and
2). if it is not achievable after concerted effort, the customer should be free to consider whether exemptions should be granted, rather than additional money spent.

PRAs are often declared to be too expensive, with some arbitrary cost being quoted as the "minimum" for a PRA. Over 40 fault tree and PRA analyses have been done at the ICPP, varying from $4K to $500K (estimate). Although it is generally true that the value of the PRA results increase with the cost, even the $4K study was well received within ICPP. ICPP's last criticality caused two years downtime. At $100 million/year operational budget, if one study a year resulted in decreasing the probability of a criticality from 10^{-3} to 10^{-4}/year, the value would be $180,000/year. This value is a reasonable expectation and exceeds the annualized cost of a PRA at the ICPP.

AREAS OF CONCERN WITH PRA: THE PRA MYSTIQUE

PRA is a magic term nowadays, sometimes considered a panacea for all safety ills. However, care should be taken that the return on the investment in a PRA justifies the cost. For example, at the ICPP, one criteria in the setting the level of quality control for projects is the requisite reliability. The design engineer is asked whether his design must meet a probability of 10^{-2} or 10^{-5}/year. Most design engineers in our business do not relate to such terminology. Such requirements would be better stated in qualitative terms.

Several times I have been embroiled in setting, or judging vendor compliance to, reliability specifications. It is not cost effective to do a PRA on every component we purchase. Often, a well specified component, or an approved buyer list, is a better way to deal with substandard components or vendors.

AREAS OF CONCERN WITH PRA: SUBJECTIVITY

PRAs are often declared to be too subjective. But, so is any analysis which tries to predict future events. For example, past criticality safety evaluations (CSEs) have considered two operators hugging equipment to make it go critical. Indeed, the results of the CSEs normally depend upon the assumptions. Also, since "gut feel" safety often directs additional spending within a project, anything less subjective is likely better than that. However, in truth, a PRA can be very subjective. Therefore, the following steps should be taken to restrict this subjectivity:

1. Understand your unique PRA problems -- If you aren't in the nuclear reactor industry, the standardized techniques may have to be changed to be less error prone (see Reference 1). For instance, at the ICPP, the initiators usually are the last event in the accident scenario, rather than the first; usually must be derived by the fault tree analysis; and are much more diverse and evolving than those within the reactor world. Such differences can lead to subtle error traps. Therefore, we find that including initiators in the fault trees is a better approach than the event tree/fault tree approach. Also, each analyst must understand the unique behavior of initiators in the plant environment.

2. Establish your credibility -- Once you understand your unique PRA problems, train your people. Then, train your peer review structure in how to trip up your analysts (and yourself) in these same problem areas. The discipline of a tighter peer review structure, and your openness in discussing potential pitfalls will greatly enhance your credibility.

3. Standardize -- Inconsistency between analysts, or analyses, cannot be tolerated. Establish an approved failure-parameters database and screen all numbers entering it. Unless you have adequate expert human error analysis support, establish a program that ensures conservatism and consistency.[2] Standardize your common cause failure analyses. (A Beta factor of 10% is used at the ICPP, but a study of our maintenance jobs database is underway to validate or change this percentage).

4. Be independent -- Never allow pressure from the design engineers or the schedule to cause the PRA results to be manipulated. The analyst must honestly feel that he can personally defend every number, gate, and assumption in the PRA.

5. Be humble -- Even though PRA is the best way to predict the future, predictive uncertainties still exist and must be allowed for. For the present, this is best handled by combining a qualitative goal, such as contingency analysis, with the PRA for a balanced safety program.

SAMPLE PROBLEM

Figure 1 shows a fault tree with "Criticality Due to Excess Mass" as the TOP event. This may be caused by any one of these four events: The process did not adequately dissolve the fuel element, insufficient poison is present in the dissolver, a fuel element with more fuel was accidentally substituted for the intended one, or two fuel elements were charged at the same time.

While at this point in the fault tree, I'd like to address the issue of assuring completeness. A well constructed fault tree is more than just a list of scenarios. It should be organized so that each gate can easily be checked to make sure the "universe" of all credible events is present for the event immediately above that gate. With this organized structure, the analyst can be reasonably assured of completeness.

For the purposes of this discussion, we are only going to develop the one event, "MisID'd Fuel Element". Under "MisID'd Fuel Element", four events are required for a criticality: The incorrect fuel ID is used, the difference between the expected and actual masses is sufficient to exceed the safety limit, the dissolver is fully reflected, and the mass is in optimum geometry.

Under "Incorrect Fuel ID used", the following probabilities are assigned:

1. "Shipper's Error" -- The shipper's QA program assigns two people to assure the correct mass is written down for each fuel element. The standard human error rate for a well-structured two-man procedure is 10^{-4}.

2. "Data Entry Error" -- Mass data is entered into the PPS by one man using the shipper's invoice. This data entry is checked by a second man, yielding a failure probability of 10^{-4}.

3. "PPS Failure" -- Once the masses are entered properly into the PPS, a computer failure can result in misidentification of the fuel element masses. This probability would have to be derived by a detailed probabilistic analysis, which we assume yields a probability of 10^{-5}.

4. "Read/Write Error" -- Before taking the fuel element to the dissolver, the operator lifts the element out of its water storage just high enough to read the identification tag attached. The probability he will make a mistake by picking the wrong fuel element is 10^{-2}.

For the misidentification error to be of concern, the mass error must be greater than 5 kg, because the failure limit is 5 kg above the operating limit. Based on the fuel mass distribution, the intended element must come from the lower 10% of the distribution, and the actual element must be from the upper 10%. The probability of randomly picking two fuel element ID's from these two portions of the distribution is approximately 4 in 100.

The expected frequency of natural flooding is 10^{-3}/year (a "thousand-year flood"). (In strict terms, this is not the actual scenario initiator, but it is adequate for the purpose of this example.)

No sprinklers exist in this cell, but water could flow in by gravity from leaks in other areas of the plant. Assume a detailed analysis has been done, yielding a frequency of once in ten years.

Humans can represent near full reflection either by "swarming" over the equipment (which is unlikely, since the uranium would have to be cleaned out of the cell prior to their entry, to reduce radiation levels), or by leaving plastic sheeting or other moderators in cell

after maintenance. A detailed analysis of this yields a frequency of once in ten years.

The amount of uranium designated by the failure limit will only go critical if it is uniformly distributed in a suspended sphere. In order for this suspension to occur, the dissolver must be agitated. Normally, such agitation only occurs once in ten batches, when the operator detects inadequate hydrogen evolution. It is also possible that more uranium could go critical without agitation (for example, 7 kgs over the operating limit), if formed in a cone. This could be dealt with in a separate branch of the fault tree, assessing the smaller probability of picking two fuel elements out of the fuel element distribution which differed by 7 kgs and assigning a higher probability for forming the cone.

REDUCING THE PREDICTED FAILURE FREQUENCY

These probabilities and frequencies yield an overall failure frequency of about 8×10^{-6}/year. Assume the following design/admin changes were recommended to reduce the frequency further (the effect of each change is evaluated in parentheses):

A. A second operator is required to independently read the fuel ID and type it into the PPS before that element is charged to the dissolver (Since this appears to be truly independent, this would reduce one of the main contributors to the TOP by 2 orders of magnitude. This would be a cost effective fix).

B. A $5 million fault-tolerant PPS has been proposed (The main contributors to failure lie outside of the PPS. Such a purchase would be a waste of money unless it affected the ability of the operators to enter the data correctly).

C. The shipper swears he has determined a brand new way to guarantee accurate values on the shipping papers, with an error rate of 10^{-6} (regardless of whether you believe that claim, this is not in the area of a main contributor, and would have little effect).

D. The fuel shipper has proposed raising the labeled values for the lighter elements so that no labeled value is more than 5 kg lower than any other (this is a relatively cheap fix that essentially makes this scenario go away. It will increase the "paper heel", requiring more frequent heelouts, and possibly resulting in a significant operational constraint).

E. The company has developed a fuel element interrogator which will determine the fissile content of each fuel element within 10% (This too will make this scenario go away, but is an expensive fix).

F. Just when you were getting excited about this new interrogator, the company tells you they cannot guarantee its availability will be higher than 90%. Also, while it effectively determines fissile content in unirradiated fuel elements, it may not do very well with irradiated fuel elements (While the true performance of the interrogator is unknown, we assume it will perform at least better than 90% of the time, for gross errors approaching 5 kgs. The real limiting factor becomes its restricted availability. Thus, we can only take credit for a factor of ten reduction in the criticality frequency).

EVALUATING PROPOSED DESIGN CHANGES

The following changes accrue after the PRA has been done initially, as Operations tries to make the plant easier and more efficient to run, or gains more experience:

A. Operations would like to install an automatic acid sprinkler system to decrease the cell decontamination time (This will increase the frequency of full reflection due to inadvertent operation of the sprinkler system. Assume inadvertent activation has a frequency of once in ten years. This would double the previously determined TOP event probability frequency. Then, the management will have to determine whether the improved operations is worth a factor of two decrease in criticality safety).

B. The plant is getting an entirely new distribution of fuel elements where the upper and lower 1/3 of the distribution are 5 kgs apart (This means about 27% of the fuel elements chosen randomly will have values over 5 kgs apart. This increases the probability frequency for criticality by a factor of 7).

C. The fuel element labels are now bar-code readable (This reduces criticality frequency by about two orders of magnitude).

D. The interrogator is proven 100% effective and can be online 100% of the time ("100% effective" turns out to mean that it didn't fail for the first 92 elements. This establishes a statistical failure rate -- at 50% confidence level --

of 2.5×10^{-3}. Since this requires adding a new fault to the fault tree, this reduces the scenario frequency by 400).

E. Someone suggested putting Boraflex around the dissolvers to eliminate the "full reflection" concern (Now we have to go back for a new criticality safety evaluation because the Boraflex introduces additional reflection that must be accounted for in computing the failure limits).

CONCLUSIONS

PRAs can be a very useful tool in setting criticality safety margins as long as careful planning goes into deciding when and how to use PRAs, particularly:

Don't allow the mystique of PRA to cause you to take on tasks which are inappropriate, or not cost effective.

Recognize the power of PRA and exert your full efforts to bring it to bear on your problems.

Structure your PRA program from the ground up (be involved in setting safety goals, and training).

Until the remaining subjectivity and predictive uncertainty can be removed from PRAs, a companion qualitative goal, such as the contingency approach, should also be employed.

REFERENCES

1. J. R. WILSON, "Practical Probability -- Initiators", Reliablity Review, Vol. 3, No. 3, (September, 1982), p. 39.

2. J. R. WILSON, P. L. SCHILLINGS, "Simplified Human Error Analysis", (To Be Issued).