TECHNICAL DIVISION
SAVANNAH RIVER LABORATORY

385729

DPST-88-423

keywords: PRA, Review

DISTRIBUTION:

J. D. Spencer, 773-A
F. Beranek, 773-A
J. P. Church, 773-41A
J. A. Smith, 773-41A
H. E. Wingo, 773-41A
D. A. Sharp, 773-41A
W. H. Baker, 773-41A
D. S. Cramer, 773-41A
D. R. Finch, 773-41A
V. E. Logan, 773-41A
D. A. O'Brien, 773-41A
K. R. O'Kula, 773-41A
S. P. Tinnes, 773-41A
A. A. Tudor, 773-41A
N. D. Woody, 773-41A
J. L. Hansen, 707-C
E. Nomm, 707-C
H. P. Olson, 773-41A
B. S. Spangler, 773-41A
J. P. Morin, 773-41A
S. V. Topp, 773-41A
D. A. Ward, 773-A
W. H. Horton (SAIC), 773-41A
Risk Analysis File, 773-41A
SRL Records (4), 773-A

TO: F. Beranek, 773-41A

March 21, 1988

FROM: D. A. Sharp, 773-41A

COMMENTS OF THE PRA SENIOR REVIEW PANEL ON THE MEETING HELD DEC. 1 - 3, 1987

INTRODUCTION AND SUMMARY

This memorandum records the minutes of the PRA Senior Review Panel meeting held at SRL on December 1 - 3, 1987, and the report on that meeting written subsequently by the panel members. The minutes are contained as Attachment 2 of this memorandum, and the report as Attachment 1.

The Panel indicated two principal concerns in their report: 1) that insufficient emphasis is being placed on the reliability data development program, and 2) that excessive detail is being built into the fault trees. These concerns have been addressed in a subsequent meeting with the Panel, held March 2 - 4, 1988. In addition, the members have been provided with a program document (Reference 1) indicating the extent, the timing, and the limitations of the data analysis effort for the PRA.

A charter was prepared for the Panel, as a followup to the request noted in Attachment 2.

Reference 1. D. S. Cramer, *et. al.*, Program to Develop Human and Equipment Reliability Data for Level 1 of the Probabilistic Risk Analysis, DPST-88-308, March 5, 1988.

ATTACHMENT 1

THOMAS D. MATTESON
1933 LITTLE RIVER ROAD
FLAT ROCK, NC 28731

January 6, 1988

Mr. David A. Sharp
Research Supervisor, Reactor Safety Research Div.
Savannah River Laboratory
E. I. du Pont de Nemours & Company
Aiken, South Carolina 29808-0001

Dear David:

I have attached a final signed copy of our comments on the Review Panel meeting held December 1-3, 1987.

This copy differs from that originally forwarded by David Okrent only because of minor editorial and typographical corrections.

Sincerely,

Thomas D. Matteson

Thomas D. Matteson

COMMENTS OF PRA SENIOR REVIEW PANEL

ON MEETING HELD DECEMBER 1-3,1987

GENERAL COMMENTS

The Panel wishes to compliment all those who made presentations to the Panel. The talks were well prepared and effective in presenting the relevant information. The Panel notes that prior to the meeting, some of the members had received only two documents for review, namely "Safety Issues at the Defense Production Reactors" by the National Research Council and DPST-87-1000, the action plan for dealing with severe LOCA issues. Both dealt with safety issues, but neither dealt directly with the current PRA. The Panel feels future meetings can be more effective if more information is provided in written form ahead of time, so that the Panel can prepare for the presentations.

The project schedule shows that final drafts of project documents are now beginning to be completed. As these become available, we think it important that they be reviewed by the Panel. This is particularly true of the event trees and accident sequence identification reports, some of which are already available.

In our judgment, the current schedule is somewhat optimistic. Experience has shown that there is usually a considerable amount of effort required in understanding the results and,especially,why unexpected results are found. Sometimes they are real, and sometimes the result of a calculational error. The resolving of such issues takes more effort than is usually realized.

In previous panel reports we have commented on the value of having the consequence code in operation before the end of level 1 and 2. We are very pleased that this has now been done. We believe that you will find this very useful as the project progresses.

For the PRA effort to continue to have a significant continuing input into the safety of plant operations, including the training and education of other personnel as the years go by, it is necessary to develop a simpler, user-friendly version of the PRA, one which is easily used by personnel other than those very familiar with the original effort. The Senior Review Panel recommends that planning for such a PRA methodology be initiated now, and that steps be taken to complete implementation of such a user-friendly PRA not too long after the current , more complex effort reaches its culmination.

LEVEL 1 ANALYSIS

The Level 1 effort includes the following tasks:
--Develop a set of initiating events
--Develop an event tree for each initiator (accident seq.)
--Determine core damage state for each accident sequence
--Quantify accident sequences (fault trees)

During the Spring meeting of the Panel, we reviewed the process by which the initiators were identified and found it to be satisfactory. The process was not discussed at this meeting; hence, no further comments are warranted.

The event trees for internal initiating events, except for the case of loss of river water, have been developed. A review of an example case showed these event trees to be of about medium complexity compared to other PRAs and to be developed following generally accepted procedures. In particular, the project developed functional event trees and then expanded them into detailed event trees, a procedure that seems to work very well. The event trees for internal initiators seem to be in good shape but, of course, the Panel has not had an opportunity to review them in detail.

The event trees for external initiators are not as fully developed as the ones for internal events. The proposed procedure for including these events seems reasonable to the Panel. However, since the plant was built, earthquake standards have been significantly tightened, so earthquakes may possibly be more important contributors to risk than in other PRAs. We urge that particular care be taken not to overlook possible seismic risk contributors.

The fault trees required for quantification of the event trees are being developed at two levels. The system trees develop a system failure down to component level faults. Then a series of component level fault trees develop the possible component failure down to basic events. In our judgment these trees (system plus component) end up being considerably more complex than the trees usually found in PRAs. They have an advantage of being able to identify some subtle dependencies that might otherwise be overlooked. They, however, require much more finely parsed data to quantify them. Given the SRP data base, we suspect this may be a problem. It may be possible to get much of the benefit of these large trees and still avoid the problem of quantification. Many PRAs have reduced their fault trees without large error by using the detailed trees to eliminate trivial branches. The detailed tree allows this to be done without accidentally eliminating branches that contain subtle dependencies. We feel some effort should be spent on developing a procedure for reducing the fault trees, or the effort required to quantify the trees may become very large.

The method of dealing with electric power, which was the source of considerable discussion in early stages, seems to us to now be handled in a very satisfactory way.

The project proposes to use the C-factor method for dealing with dependent failures. However, the detailed fault trees also have boxes identified as dependent failures. Care must be exercised to be sure no double counting results from this procedure. Discussion with the staff indicated that they were aware of this problem.

The project has widely used "flags" or inhibit gates in the development of the fault trees. We strongly endorse this procedure as a way of permitting one fault tree to be used to represent a number of similar situations.

The fault trees, with the exception of the issue discussed above, seem to be coming along very well, based on our cursory review.

LEVEL 2 ANALYSIS

This was the first meeting at which the Panel heard about the planned approach , schedule, and progress-to-date on Level 2 analysis for the PRA. The Panel believes that the proposed "flowchart" methodology, rather than a fully mechanisitic code, is a reasonable choice in view of the overall schedule for the PRA and the start date for significant effort on the development of the Level 2 approach. The combination of modeling, physical intuition, and engineering judgment should be acceptable, if careful attention is given to documentation of the alternatives deemed plausible at each stage in the analysis of scenarios, and if adequate discussion is included concerning the reasoning involved. Clearly, the gaps in knowledge are large, and the imprecision in modeling and the uncertainties in subjective judgment will be significant.

The planned later advent of a mechanistic code for predicting the Level 2 course of various accident scenarios (to be developed under the Severe Accident Assessment Program, SAAP), will be useful in a future round of efforts to improve the PRA's sophistication and accuracy. However, with or without the mechanistic code, the PRA effort should include a concerted effort to identify, describe and quantify, as practical, the uncertainties involved.

The Panel recommends that an increasing number of SRL personnel should become knowledgeable about the phenomena involved in Level 2 analysis.

As with the Level 1 effort, the Panel believes that the proposed schedule for the completion of the Level 2 effort is somewhat ambitious.

Some more specific comments concerning the planned Level 2 work are given below.

1. It seems possible, if not probable, that one or more additional demonstration initiators will be needed beyond the three currently identified. For example, a sudden large reduction in coolant flow, coupled with a failure to scram, might result from a severe earthquake. The phenomenological course of this scenario may be enough different from the first three to warrant its study. Similarly, certain interrupted flow accidents may lead to important differences in fuel motion and dispersion.

2. The fuel element melting accident which occurred at the Westinghouse Test Reactor should be looked into for possible relevant empirical information.

3. The potential role of fission product gases in the modeling of early fuel element melting and failure should be evaluated.

4. The transition from early meltdown of a single subassembly to what occurs during large scale meltdown will have to rely heavily on engineering judgment. It is important that this aspect be treated in preliminary fashion as early as is practical, in order to permit a maximum exchange and cross-fertilization of ideas and opinions. The same considerations apply to "late melt relocation".

5. Since relatively modest in-vessel fuel-coolant interactions (steam explosions) may have an important effect on the relocation of fuel or even the induction of supercriticality, this phenomenon will require careful attention.

6. The matter of aerosol generation should receive careful scrutiny. The PRA group should stay in close touch with the experimental program planned under SAAP.

7. The recriticality program element may pose questions which are dificult to resolve, particularly with regard to the estimation of the likelihood of a really significant event. Again, it would be useful to attempt a preliminary estimation early, in order to permit considerable time for examination and reexamination of the ideas proposed.

DATA ANALYSIS

A General Comment

The Panel feels there may an inclination to consider the effort to produce quality failure information to be of considerably less importance than the design of the analytical structure that will use it. (This situation is ~~not~~ unique.) Reliability information has often been a profuct of "data collectors" rather than users. The data collectors often have different objectives than users, usually resulting in piles of reports designed by computer programmers having no knowledge of the users' needs, and having important integrity problems, as well.

The Panel encourages continuing efforts to ensure that, for the items of importance to safety and to operating cost, the process for determining the failure probabilities to be used in the PRA and the process for monitoring experience not be second class.

These comments are not intend to turn SRL in the direction of more elegant statistics, rather that they focus attention on the quality of the inputs and the simplicity and integrity of the outputs provided to users.

Reliability Data

The success of achieving a "user friendly" PRA will depend not only on its design but also on the ongoing availability of contemporary component/subsystem reliability data.

An objective of the Level 1 activity should be to identify ranked lists of components and subsystems whose functional failures are the largest potential causes of core melt. The list of ~~Some~~ components may contain perhaps 100 items (including some repeats of the same component used in different subsystems/environments). The subsystem list would be much smaller. These lists should form the foundation for an ongoing process of collection of degradation, failure, and in a few cases, life data.

Note that this suggestion differs totally from the usual interests of reliability analysts serving a design community. Much of what is being done in the LWR community is based on these design interests. Systems designers are primarily interested in collection of failure rate data without attention to the definition of failure, proximate cause or, in some cases, criticality. They want to know what they feel is necessary to improve future designs, not what the current user must know to optimize his operations.

In addition to the "active" system components, it is important to identify the critical structural components, or Structurally Significant Items" (SSI), static items whose failures are caused by loss of strength from fatigue, erosion, corrosion, etc. Experience has shown that such failures tend to be concentrated at specific locations and have some dominant cause based on the design, the materials used, the environment, etc. These failures are usually progressive, and their prevention requires some regular inspection/test to determine their condition. (If measureable degradation is not a precursor of failure, then some life limit based on the results of off-site tests is required.)

Having identified the objects of interest, the next requirement is to identify the data which must be collected.

1. Most reliability data systems are designed by "data collectors", not end users. Data collectors often perceive data as an end product. This perception usually results in unfocused, unwieldy, costly misinformation.

2. Many reliability data systems fail to incorporate features in their design that (1) record all the failures of the items of interest, (2) correctly identify the failed unit, (3) identify the cause of failure - shop finding, (4) accurately capture the related experience - the denominator, (5) limit the scope to items of importance.

The lists previously described can be used to limit the scope of the data system. They can, further, provide the basis for a hierarchy that collects elementary information (permitting simple failure rate calculations) on all items, additional information such as conditions found and corrective action (permitting item level engineering analysis) on a smaller set of items, and last, life data (permitting age-reliability analyses) on a small set of costly, critical hardware.

The largest data set should be selected to support the updating of the "user friendly" PRA. The middle set should be selected to support maintenance management and the interests of the engineers responsible for support of that activity and for hardware improvement. The smallest set should focus on understanding the age-reliability characteristics of critical hardware for which the threat of infant mortality or requirements for costly periodic overhauls should be examined and understood.

Definition of Failure

The ability to compare failure rates of units whose failures are determined by measuring performance or condition against some standard is a particular problem that most reliabilty data bases fail to address. Several facts must be in hand. First, the standard must be clearly defined, not left to the judgment of individual observers. Second, the standard must be part of the operations or maintenance instructions and be the specific basis for initiating corrective actions. Third, the standard should be based on a degradation analysis so that it has a rational basis, one that considers the specific environment and function, not simply adherence to some number on a drawing used for manufacture.

The purpose of these standards is to avoid unnecessary adjustment or replacement actions while ensuring that, for critical functions, adjustments or replacements are made before functional failure occurs. The frequency of such will, of course, be related to the degradation rate, accessibility and the confidence one wishes to have that functional failure will not occur.

Reporting

A periodic reliability report presenting the failure experience of the identified items should be designed. It should show the mean failure rate currently used in the PRA and a time-series representation of the experience to date. Because of the relatively slow rate at which experience is acquired, annual publication of this report should suffice. It would, however, be useful to build the data base contemporaneously and, for each item, establish a failure rate above the mean used in the PRA at which an exception notice would be auto-generated for that item.

David Okrent Norman C Rasmussen

Thomas D. Matteson David Okrent Norman C. Rasmussen

December 23, 1987
Revised - January 4, 1988

ATTACHMENT 2

cc: F. Beranek
PRA Group
W. H. Horton
PRA Files

January 8, 1988

<u>MEMORANDUM</u> RSRD-RD-054

To: D. A. Sharp
From: S. V. Topp S.V.T.

QUESTIONS AND ANSWERS FROM SENIOR REVIEW PANEL

Following are exchanges with the Senior Review Panel at the December, 1987, meeting, as reviewed and edited by the persons involved.

Okrent to Beranek: Do you think you really know where industry is in terms of risk, when you say you want the PRA to compare SRP with industry? Industry usually has two numbers for residual risk--one from their PRA, and one from an NRC assessment of their PRA, and the two can be orders of magnitude different.

Okrent: We should have a written charter for what the Panel should be doing.

Okrent to Sharp: Why is the Severe Accident Analysis program different from Level 2 of the PRA?
Sharp: The SAAP is an extension and improvement of Level 2 methodology.

Okrent to Sharp: How much further do you expect the seismic program to go?
Sharp: We plan to redo the seismic analysis during the Level 1 work.

Okrent to Sharp: What are you going to do about aerosol

impact on filters, per NAS report?
Sharp: Phase 1 considered heat load, but not aerosol blockage; we will use the CONTAIN code to model aerosols in the Level 2 work.

Okrent to Wingo: How is seismic study going to tell whether the 105 building settles unevenly during liquifaction?
Wingo: Probably through judgement, but we are looking at the issue now.

Okrent to Wingo: Could an earthquake cause a fire from hot shorts--maybe in cable trays?
Wingo: We haven't looked at that yet.
Okrent: What about a fire propogating through the ventilation system?
Wingo: Probably not because air flow is away from the control room toward the process room.

Rasmussen to Horton: What if you think you isolated a big leak, but you really hadn't been successful?
Group Discussion: We don't have that modeled now.

Okrent to Topp: What are we doing about operator response to confusing and contradictory alarms or instrument indications?
Topp: We haven't modeled any yet, but will probably depend on time reliability correlations for any we can think of, if we can estimate the time the operators would have to respond.

Matteson: What about low voltage changing the order of relay action, or causing relay chatter? That is, a low probability initiator could cause a high probability instrument and control failure.
Tudor and Cramer: We are looking at this.
Topp to Matteson: Is there any good way to find out other than functional tests?
Matteson: That's the only way I know of.
Topp: If we can identify any, I suppose we could only worry about those the operator has time to do anything about, like close a valve manually.

Matteson to Logan: Common cause failure is not the same as dependent failure. In most cases, our "dependent failure" should be changed to "common cause". Dependent is covered by the detailed modeling in the fault trees. Dependent is when failure of one component triggers failure of another component.

Topp: We `agree, and we should change our jargon.
Horton: Our fault trees are developed so much already that we will have to stay with the present jargon.

Okrent to Sharp: Will the PRA in two years be user friendly for future studies?
Sharp: Yes, but we anticipate some difficulty in accomplishing this.

Davis to O'Kula: Are you considering isotopes other than iodine, like cesium and tellurium, for in-vessel transport? q
O'Kula: Yes, the others are there too.

Okrent to O'Kula: What fraction of the core iodine would the filters handle with no bad effects?
Sharp and Baker: At least 5%, proabably more like 15%, without the sprays.

Davis to Amos: Why not drop the sequences with single rod withdrawal as initiator because of their low contribution to risk? (Low probability of scram failure.) The LWRs write these off on the basis of probability.
Amos and Sharp: Because (1) these sequences may propagate to high consequences, (2) they are needed to give information on recriticality, (3) this is probably the only way we can get an in-vessel steam explosion, and (4) we need this for completeness of the PRA.

Rasmussen to Sharp: All past accidental criticality yields have been within about a factor of 10 of each other. Do you expect recriticality to be any different?
Sharp: No, but we want to try to establish a specific "best estimate" yield and not utilize an overly conservative upper bound yield. Therefore, we don't want to just assume a fixed yield.

Okrent to Sharp: How are uncertainties going to be handled in Level 2?
Sharp: We haven't decided how to handle uncertainties beyond Level 1 yet.

Okrent to Sharp: Is the PRA going to cover reactor changes that are committed but not implemented yet?
Sharp: No, it will cover the status as of June 1987, except for the fourth addition system. This system is being

installed now. If the fixes to the ~~R~~PCS expansion joints are done promptly they may be included also.

Okrent to Sharp: What about the proposed seismic restraints?
Sharp: The PRA will probably be done without those because the sehedule for installation is not yet finalized.

Okrent to Sharp: Most commercial PRAs include changes that are planned and committed but may not be in place for as much as 2 years.
Sharp: We believe the credibility of our PRA may be damaged if we include systems and changes that are not installed.

Okrent to Sharp: Incidentally, why do things take so long, like the seismic bracing of batteries and motor control centers?
Sharp and Wingo: Partly because of the complex, slow design, cost, approval, and installation process including Wilmington engineering, and partly because we are into lengthy QA requirements. The seismic bracing project is no different in this regard than are other large, expensive reactor improvement projects on the site. Typically, such projects take years do.

Okrent to Sharp: Do we plan to have another contractor to develop a" second opinion" on Level 2 methodology?
Sharp: No, but we are open to suggestions from the Panel.
Beranek: In the severe accident program we are getting help from Battelle Columbus on phenomenology and chemical interactions in time to consider before completion of PRA in the summer of 198~~8~~9.

Rasmussen to Beranek: Will you see that the Battelle work is coordinated with the Level 2 PRA?
Beranek: Yes.

Rasmussen to Group: Do you count dependencies twice by using C-factors and modeling dependencies low in the fault trees?
Topp: Gave numerical example using dependent and independent maintenance errors on a valve.
Rasmussen: O.K., I'm satisfied you're being careful enough.

Okrent to Topp: Are you using your best efforts to think of acts of commission and acts arising out of confusing information from the instrumentation?

Topp: We will be using our imaginations where we can, and also perhaps the Simulator will give us some hints on where to look further.

FOLLOWING FROM THURS PM COMMENT PERIOD

Rasmussen: Since the Panel found one event tree that could use a change, they think there may be others, so QA of event trees is important.
Sharp: We agree. We have review within the PRA group, plus peer review in SRP.

Rasmussen: More careful thought should be given to event trees from earthquakes as an external initiator.

Rasmussen: We should be able to simplify the fault trees more--we can't get data in the detail implied now.

Davis: You may want to look at the binomial failure rate model if there are more than two dependent systems--say three of four.

Rasmussen: The Level 1 schedule is too optimistic. Sequence analysis will uncover a lot of changes to be made in models and data. This was a time-consuming business in the RSS, and it will be in this PRA too.

Matteson: In order to make the PRA user friendly, we should think of ways to easily input new data as we get more in-service experience. Update of data should be a living process to account for aging, etc.
Cramer: We will establish a schedule for updates.

Matteson: We should look at data in recent industry PRAs, but not through INPO, because INPO filters too much of what the underlying failure causes are, and never say what the definition of failure is. We could try the industry AEOD reports (Analysis of Equipment Operating Data). We might identify failure modes this way that have not occurred here yet.

Matteson: We are now in a position where we can begin to understand aging. We should follow up on aging--but only on a selected number of important items.

Okrent: Yes, you should try harder to think of new aging failure events.
Tudor: We have Bill Vesely coming to show us how to identify the important ones.

Okrent: Level 2 is a hard problem. I think you won't be able to predict what you will be able to accomplish by 1989. If you try, you will be vulnerable to incomplete technical treatment if you are not flexible in changing your schedule as you learn more.

Okrent: We should look up the Westinghouse fuel melt in the late 1950s, and try to benchmark our releases. See Thompson and Vessly, Volume 1, Chapter 13 (MIT Press).

Okrent: A charter for the Panel should be written .

Matteson: We should consider using C reactor for tests that we wouldn't otherwise be able to do.