IAEA-TECDOC-522

A PROBABILISTIC SAFETY ASSESSMENT PEER REVIEW: CASE STUDY ON THE USE OF PROBABILISTIC SAFETY ASSESSMENT FOR SAFETY DECISIONS

A TECHNICAL DOCUMENT ISSUED BY THE
INTERNATIONAL ATOMIC ENERGY AGENCY, VIENNA, 1989

LIST OF PARTICIPANTS

Authors

USA

R.J. Budnitz H.E. Lambert	Future Resources Associates Inc. 2000 Center Street Suite 418 Berkeley California 94704

Oversight Committee for the Development of a Series of PSA Case Studies

FRANCE

A. Carnino	Electricité de France 32, Rue de Monceau 75384 Paris CEDEX 08 France

GERMANY, FED. REP. OF

P. Kafka	Gesellschaft F. Reaktorsicherheit (GRS)mbH Forshcungelände 8046 Garching

SPAIN

J. Villadoniga	Consejo de Seguridad Nuclear S/Sor Angela de la Cruz 3 28020 Madrid

United Kingdom

S. Hall	Systems Reliability Directorate UKAEA Culcheth Warrington WA3 4NE

USA

J. Gärtner	Electric Power Research Institute Palo Alto California 94303

O.E.C.D/N.E.A.

J. Caisely	Nuclear Energy Agency O.E.C.D./N.E.A. Paris

IAEA

M. Cullingford S.M. Shah	Scientific Secretary

A PROBABILISTIC SAFETY ASSESSMENT PEER REVIEW:
CASE STUDY ON THE USE OF PROBABILISTIC SAFETY ASSESSMENT
FOR SAFETY DECISIONS
IAEA, VIENNA, 1989
IAEA-TECDOC-522
ISSN 1011-4289

Printed by the IAEA in Austria
October 1989

FOREWORD

Probabilistic Safety Assessment (PSA) can provide important information related to the spectrum of possible accidents for a particular Nuclear Power Plant or other industrial installation. Such information, when based upon reliability data obtained from experience with that particular plant, concerns the accidents leading to core damage, the human system and component failures which constitute these accidents and the safety level of the plant. Following the accident at Three Mile Island in the USA (TMI-2) and more recently at Chernobyl in the USSR, PSA was used to understand how these accidents happened.

The demand for activities within the Agency's PSA programme has increased, particularly in the area of application of PSA insights to safety decisions.

Consequently, an Advisory Group Meeting (AGM) was held on "Development of Manual for Probabilistic Risk Analysis and its Application to Safety Decisions", in Vienna, Austria, on 14 - 18 May 1984. The AGM has identified as a need documented experience with application and utilization of Probabilistic Safety Assessment. It was recommended that a series of case studies be written documenting actual experience where PSA has been used to give guidance in safety decision making. The first peer review on each of the case study was to be carried out by technical experts, and a high level peer review would be carried out by a senior oversight group. Based on the recommendation of the AGM a programme to publish a series of case studies on the use of Probabilistic Safety Assessment for safety decisions was initiated.

The Agency requested a number of scientists and engineers to document, in a uniform and suitable format actual experience with the application of PSA to safety decisions. A number of institutions' analysts such as NRC, NSF, EPRI, Argonne National Laboratory in the US, GRS (FRG), EdF (France), CSN (Spain), SRD (UK), AEA (UK) and OECD/NEA participated in the programme. To ensure the quality of case studies peer review was needed. A number of highly qualified experts in the field of Probabilistic Safety Assessment agreed to participate in reviewing case studies developed within this programme. The experts met on a number of occasions under the title of Oversight Committee to review and comment on the draft versions of various case studies as they were completed. The review comments were sent to the authors and incorporated in the case studies. In some cases this process was repeated more than once.

In this case study the PSA had examined the Shoreham Nuclear Power Station, owned by Long Island Lighting Company, the PSA sponsoring Utility on the North Shore of Long Island, New York. The case study references other PSA literature on peer review which helps put this case study in perspective. One such reference, An Intensive Peer Review for PRA [ref 4] in fact contains a fully-documented case study of a peer review for a level 3 PSA. The reader is encouraged to refer to this Nuclear Safety Analysis Center report, available through the Electric Power Research Institute as the NSAC-67 report.

The issues that are emphasized in any specific review will be influenced greatly by the organization sponsoring the review and by its specific objectives. In this case study, for example, the sponsor was interested in the technical basis of evacuation planning for the spectrum of accident scenarios that could occur. Therefore, the review focussed upon characterization of potential releases. Another review, even for the same PSA might logically focus on characterization of core damage sequences rather than radioactive release and might focus more on the accuracy and uncertainty of frequencies and probabilities. In general, it is believed that the characterization and relative frequency of core damage accidents would have the greatest interest in most PSA reviews.

The Oversight Committee is satisfied that this case study is an accurate and useful description of what was done in the study and of how it was done. In several areas the report does not, however, explain why a specific decision was made. For example:

- How was it decided that the level of effort allowed by the budget was adequate?
- Why was it acceptable that certain technical areas were not within the specific expertise of the reviewers?
- How were the topics for detailed review and level of review determined?
- On what basis were some topics chosen for separate analysis?

As with all case studies in this programme this is an example application of PSA to safety decisions. The IAEA has another programme to produce "Guidelines for conducting PSAs of NPPs". These guidelines address the methodology, management, and documentation necessary, in two levels - general guidelines and specific guidelines. These guidelines should give answers to the questions listed above. The reader of the case study should keep this in mind since the guidelines will deal with all the aspects of a peer review while the case study deals only with a real example dedicated to a specific application.

CONTENTS

1. INTRODUCTION

The purpose of this case study is to illustrate, using an actual example, the organizing and carrying out of an independent peer review of a draft full-scope (level 3) probabilistic safety assessment.

The PSA, [ref 1], had examined the Shoreham Nuclear Power Station (SNPS), a large new boiling water reactor, owned by Long Island Lighting Company (LILCO), the PSA sponsoring utility, on the north shore of Long Island, New York. SNPS is a BWR-4 with a Mark-II containment. The PSA study had been completed in draft form by the PSA contractor. The plant in question was in its final year of construction and was thus available for a thorough walkthrough.

The peer review [ref 2], was sponsored by the local governmental entity, Suffolk Country (New York). The sponsoring body was responsible for developing a plan for emergency protective actions, in case of an accident at SNPS, and wanted the independent peer review in order to ascertain whether the utility sponsored PSA could be used as an acceptable technical basis for evacuation planning. In order to carry out the peer review, the review sponsoring body selected independent contractors who worked under the direction of its own administrative staff.

The purpose of this case study is to illustrate, based on an actual example, the issues that can arise in organizing and carrying out a peer review of a large, full scope PSA. The specific findings of the peer review are of less importance than the approach taken, the interaction between sponsor and study team, and the technical and administrative issues that can arise during a peer review.

This case study will examine the following issues:

- how the scope of the peer review was established, based on how it was to be used by the review sponsoring body;
- how the level of effort was determined, and what this determination meant for the technical quality of the review;
- how the team of peer reviewers was selected;
- how the review itself was carried out;
- what findings were made;
- what was done with these findings by both the review sponsoring body and the PSA analysis team.

Because the peer review took place after publication of the draft version of the PSA study, there was an opportunity to affect the content and conclusions of the final SNPS PSA report. The case study will discuss how the peer review's findings affected the final version of the PSA, and why. Sometimes a peer review is undertaken at an earlier stage, such as while the study itself is still in progress. In such a situation, there is even more opportunity to affect the PSA's overall approach and results.

The key technical finding of the peer review was that the PSA had been conducted at a level of competence that was equal to the state of the art at the time the study was completed (which was mid 1982). However, the review group identified a few areas where the technical analysis could be improved or where the analysis was apparently erroneous. These will be discussed in more detail below.

The PSA literature contains a few pieces of guidance that may be of interest to those planning a peer review. (The reader should note that the abbreviation "PRA" for "probabilistic risk assessment" is used in much of the earlier literature in place of the abbreviation "PSA" that is used here). The most thorough piece of guidance is the recent Brookhaven report, [ref 3], PRA Review Manual, which describes in great detail the steps to be undertaken in a full review. However, the level of effort required to carry out a review of the kind described in the Brookhaven report is very large, between 3 and 4 person-years of effort, whereas the review carried out in this case study required about 5 person-months. With 3 to 4 person-years of effort, a much more thorough review is feasible, including repetition of many important analyses.

A second recent report, completed for the Nuclear Safety Analysis Center at the Electric Power Research Institute, EPRI, by Delian Corporation, [ref 4], is An Intenstive Peer Review for PRA. This report provides useful guidance on how to structure an intensive review, in which a few analysts devote about two weeks full-time to intensive interaction with the PSA study team. The guidance on how to structure peer review technical topics is very useful.

The Nuclear Regulatory Commission-sponsored PRA Procedures Guide, [ref 5] also contains some guidance on peer review, but it is quite general.

These three references [3,4,5] discuss very different types of peer review. A peer review of a multi-person-year, full-scope PSA can accomplish much more, obviously, if several person-years are devoted to the review than if only several person-months are available. Generally, however, a review that devotes much less than a few person-months cannot be expected to provide useful coverage of all of the major topics in the study.

2. HOW THE SCOPE OF THE PEER REVIEW WAS ESTABLISHED

The scope of any peer review depends fundamentally on the objectives of the sponsor. These objectives can range from a desire for a thorough, detailed technical review of the entire PSA study to a broader, high-level review that studies whether or not the analysis has been accomplished competently. Also, the objectives of the review depend on the application that will be made of the PSA study. One key lesson that the study team learned is that the review must be focused on the sponsor's intended application of it.

In the case under discussion, the review sponsoring body had a legal obligation to develop a plan for emergency protective actions in case of a large accident at the reactor facility. Therefore, their central need was for insight into whether or not the releases calculated by the PSA accurately reflected the best information available. Because the PSA categorized the accidents at Shoreham into five 'release categories' (which were called "generic accident sequence classes" in the PSA), one central objective for the peer review was to study whether this categorization was technically justified, and whether the sequences were appropriately binned. (The reviewers' conclusion was affirmative).

The second central objective was to study the calculation(s) of core melt frequency for each of these classes, in order to determine if the calculated frequencies were technically correct. The third central objective was to study the accident phenomena (physics and chemistry of core melting, behavior of vessel and containment, etc.) of each of these classes, in order to determine whether or not the modeling and data used supported the conclusion about containment failure probabilities, timing and energy of the calculated releases, and release fractions of various radionuclides.

The review sponsoring body staff had a fourth central objective as well, which was to review the calculations of offsite consequences given the radionuclide releases. However, this part of the review was carried out by a different contractor, [ref 9]. There were substantial exchanges of information between the two review efforts, and the coordination was excellent - but this stemmed largely from a prior working relationship between the two review team leaders and would not necessarily be true in general. The review team believes that it is usually preferable to carry out the entire review as one project to avoid possible problems, even though no problems occurred in the peer review effort discussed here. This would mean placing one individual in charge of the entire review, to provide a single point of responsibility and authority for the whole effort, and a single point of contact with the sponsor.

The scope of the peer review, in summary, was established to carry out the first three of the four central objectives cited above. As stated earlier, these objectives were needed to provide review sponsoring body staff with information about the magnitudes, probabilities, and characteristics of potential large accident releases from the Shoreham nuclear power plant.

Because of the nature of the review sponsoring body's task (preparing an emergency plan), its staff asked that the reviewers pay more attention to the characterization of potential releases than to the calculations of the probabilities of their release, or to the consideration of issues related only core damage.

3. HOW THE LEVEL OF EFFORT WAS DETERMINED AND ITS IMPLICATIONS

The amount of support available was constrained due to budgetary limitations, which is a situation often encountered. The funds available were sufficient to support about five person-months of professional effort for the peer review, not including the separate contract for the review of the offsite consequences analysis.

In the initial discussions between review sponsoring body staff and the review team leader, the first issue faced was whether or not this amount of effort was adequate to perform a reasonable independent review. An early determination was made that the support would be adequate. It is important to recognize, however, that there was a compromise made in the beginning of the review project, of the following character: the review effort would not be able to undertake substantial independent analysis to verify the validity of the many calcuations in the PSA, but would rather be limited to reviewing only a few (judiciously selected) areas in detail, with other areas reviewed only in an overview sense.

The five-person-month level of effort was sufficient, as it turned out, to perform such a review, and this review did include some independent analysis. The much deeper review that was not undertaken, involving much more extensive independent checking on the PSA work, would have required 3 to 10 times more resources; 1 to 4 person-years! The adequacy of the level of effort used was, of course, not known in advance, because it could not be known in advance whether or not any key safety issues would turn up that would require major additional review work.

The implications of the level of effort available were carefully explained to the sponsor, so that the review sponsoring body staff would have the same expectations as the review team concerning the breadth and depth of the review to be undertaken. This is a crucial step: whenever there is a gap existing between the expectations of the sponsor and the resource-limited capabilities of the review term, dire consequences may result for any review. Fortunately, there was no gap in expectations between the two groups in the review process under discussion. The success of the review in meeting the review sponsoring body's needs was in a major way attributable to the care taken in the early stages to achieve a mutual understanding on this issue.

4. HOW THE TEAM OF REVIEWERS WAS SELECTED

There were two considerations involved in putting together the review team:

- the team should possess technical competence in all of the technical issues to be covered in the review;

- the team should be 'independent' i.e., without real or perceived conflicts of interest.

The team leader, who was given full responsibility for assembling the review team, decided to assemble a team of four reviewers, selected to cover the main areas that in his judgment required review. The judgment was made that using a larger number (e.g., six or eight reviewers) would provide too little support for each individual reviewer, while using a smaller number (e.g., only one or two reviewers) would have limited the coverage of technical topics. There was nothing special, however, about the number four; three or five would have been equally acceptable, depending on the specific individuals selected and their breadth of expertise. Indeed, one of the authors recently participated in another successful PSA review in which seven reviewers used about the same level of effort, but the review scope of the study was slightly narrower. The selection of the number of reviewers per se is not the main issue. The team members should be chosen for their individual expertise, with consideration for the extent to which these areas of expertise may overlap. One must start by considering the individuals and build the review team as a unit.

The technical areas covered by the review team were as follows:

- the team leader had competence in both systems analysis and source-term/phenomenological analysis;

- one team member had very strong expertise in systems analysis;

- one team member had extensive experience in thermal-hydraulics and core-melt phenomena;

- one team member had strong backgrounds in both systems analysis and evaluation of containment performance, including fission product deposition and transport.

Certain areas of expertise were not fully covered. These included the area of evaluating the input data (failure rates, initiating events, etc.); the area of human factors modelling and human error rates; and the area of quantification of uncertainties. Among the review team members, however, there was enough expertise in each of these subjects to provide a reasonable level of review. No key topics went un-reviewed, although the depth did vary from one topic to another. This is another situation in which the considered judgment of the team leader is crucial. There is no substitute for this kind of judgment, because it is impossible to review in equal depth every aspect of a complex, full-scope PSA. Therefore, some experienced judgment is always needed.

Independence was another important factor in the selection of review team members. No review can be fully adequate unless the reviewers have enough independence.

- There must be independence in the sense that no reviewer is reviewing his/her own work, either directly or substantively. This includes indirect aspects of the work. The review could be compromised, for example, if a reviewer had been involved in developing the models, data, or codes used in the analysis.

- There must be independence in the sense that the reviewer is not beholden to any interested party, i.e. the reviewer cannot be in a position where he/she is reluctant to make a negative comment for fear of future loss, either financial loss or loss of stature, friendships, or working relationships.

- There must be independence in that the reviewer is not tarnished with a reputation (either deserved or undeserved) for taking prior positions on issues based on non-technical considerations. This is a tricky point and involves a subjective judgment on the part of the sponsor and/or team leader.

Unfortunately, today it is almost impossible to satisfy all aspects of the 'independence' requirement in undertaking a PSA review. This is true because the PSA community is so small that almost all analysts know each other. Inevitably, some members of the study team whose work is under review will have at least some measure of compromised independence with almost any review team that might be assembled.

In the specific case under discussion, there were several compromises of 'complete independence', but all were judged to be minor. For example, one reviewer had previously reviewed an extensive report done by the PSA team, so that he might be accused of simply repeating old disagreements. Another reviewer had been the principal proponent of an analysis method considered in the PSA community to be the 'rival method' to the one under review. Still another reviewer had been on the NRC regulatory staff a few years earlier when decisions affecting the plant design had been made; he might be accused of reluctance to criticize a reactor design that reflected his earlier regulatory involvement.

All of the potential 'compromises of independence' were judged to be too peripheral (and the personal integrity of the reviewers judged to be too staunch) for these issues to be considered significant. However, issues of conflict of interest are always subjective in the end!

5. HOW THE REVIEW ITSELF WAS CARRIED OUT

The review process itself involved the following steps:

1) Receipt by the reviewers of the draft PSA report, plus back-up documentation on important aspects of the analysis;

2) An initial set of meetings of the reviewers to delineate individual areas of emphasis, areas where two or more reviewers should interact, and levels of effort to be directed to investigating various issues;

3) A site visit during which the review team toured the reactor site, asked relevant questions, obtained needed information from the utility and its contractors, and decided which issues required in-depth review;

4) A second team meeting in which key issues were discussed again;

5) Interaction with the PSA analysis team, mainly on an individual basis in which one reviewer interacted with one analyst;

6) Review work by the individual team members, leading to the drafting of individual sections of text as contributions to the final peer review report;

7) Circulation of the individual sections among the other reviewers for technical comment and editorial consistency;

8) Revision of the drafts by the individual authors, based on technical and editorial comments;

9) Integration of the separate sections into a 'final report' under the guidance of the review team leader;

10) Circulation of this version, labelled the 'draft final report', among review sponsoring body staff for comment;

11) Publication of the 'final report'. (There were no comments from the review sponsoring body staff, so the draft and final versions were identical.)

Obviously, the key step is the planning step, in which it is decided which topics should be reviewed and at what level of detail. In the case study under consideration, this occurred during the early meetings of the review team. The structure was worked out by the reviewers on an ad hoc basis.

Today, a team of reviewers can utilize either of two well-documented guides that set down how to structure the technical parts of a review: the Brookhaven PRA Review Manual, [ref 3], and the Nuclear Safety Analysis Center--EPRI guide [ref 4]. Both of these references give specific guidance. As an example of the level of detail provided, the interested reader can refer to Appendix A of this case study, in which two pages are taken directly from the Brookhaven report. These two pages provide the general characteritics of any peer review.

The main non-technical issue involved in carrying out the review was access to the relevant technical information. Specifically, the review sponsoring body's desire for 'full independence' coupled with the existence of an adversarial process then underway (the operating license hearing before an

NRC Atomic Safety and Licensing Board Panel), produced an original constraint that the peer review team not interact on a personal basis with the PSA analysts! The only interaction was to be through study of the written material that was provided. The review team accepted this pre-condition reluctantly and vigorously stated its opinion that the review would be substantially more effective if full person-to-person access to the PSA analysts were allowed. After only a few weeks of discussion, the restrictive condition was removed by the review sponsoring body and numerous conversations and meetings took place between reviewers and analysts.

The peer review team had access to and used not only the full draft PSA itself, but also numerous supporting documents such as fault trees and input data. The cooperation of the PSA contractor analysis team and of the PSA sponsoring utility personnel was outstanding. In retrospect, the review team believes that the quality of the review would have been seriously compromised if access to the original analysts had been denied. This is another crucial piece of guidance in carrying out any peer review on a complex study such as a full-scope PSA.

The interactions with review sponsoring body staff were infrequent and fully satisfactory. Its staff had very little background in the technical issues involved and provided no interference of any kind. After the scope of the work was established during an initial meeting that provided both parties with a full understanding of the time schedule, the review sponsoring body staff simply sat back and waited for the draft report. It was circulated to interested staff members and other review sponsoring body contractors (e.g. their emergency planning contractors) after which it agreed that the report should be published in final form without modification. It is recommended that peer reviewers take care to ascertain whether or not significant interference might be expected from the sponsor, and to make efforts to minimize it.

There are often tensions between utilities and regulatory bodies which can interfere with carrying out a fully satisfactory technical peer review. This cannot be allowed. For example, non-technical problems can prevent useful dialogue between reviewers and at least some sources of relevant technical information. Sometimes, a peer review sponsored by a utility to examine its own utility-supported PSA study may suffer from some of these restrictions, since the utility may wish to keep the PSA results or analysis from the regulators until it suits their licensing 'strategy'. This peer review was not impeded by such problems.

6. WHAT FINDINGS WERE MADE, AND WHAT WAS DONE WITH THEM

The introductory section of this paper has already given the key technical finding of the peer review, which was that the draft PSA had been conducted at a level of competence equal to the state of the art at the time (mid - 1982) that the work was done. The basis for this fundamental finding was the peer reviewers' familiarity with the then-current state of the art of PSA, and their understanding of what the draft report contained. This fundamental conclusion is the most important by far and is what gave the reviewers the confidence that it was not necessary to study every detailed calculation in the overall analysis to check the validity of the numerical results. (By contrast, suppose that the conclusion had been the opposite: suppose that the PSA analysis had been much behind the then-current state of the art, in terms of either data used, models employed, or execution of the study. In such a case, the reviewers would be unable to affirm the validity of the broad results).

It is important to recognize that this fundamental conclusion, usually sought by the sponsors of any peer review, cannot be affirmed unless the reviewers are truly up-to-date themselves. This means that the review team must be comprised mainly of practicing analysts. It is also very important that the sponsor insists on a fully-documented report from the peer review group, as was true in this case study. Documentation of any response to peer review comments by the analysts is also important.

The general finding of the peer review team was supplemented by a great amount of technical detail in their report (which was about 200 pages long: a 65-page main report and a 135-page appendix, [ref 2]). In these 200 pages the reviewers discussed a number of technical issues, either where there was a disagreement or where the review team performed separate analyses that provided additional insights on selected safety issues. The selection of the few topics for which separate analyses were undertaken was an important step, because it was crucial that the peer reviewers concentrate their effort on the most important topics. Here the judgment of the team leader was a key ingredient in the success of the review work.

A few of the reviewers' comments were in the nature of confirming the validity of the PSA analysts' approach by carrying out a different analysis using different models or assumptions or data. Other reviewer comments pointed out what were thought to be errors or inadequacies in the models used. In one case, there was a full reanalysis of a detailed issue that revealed an apparently erroneous assumption. Still other reviewer comments discussed how known conservatisms present in the analysis might be removed. Removing these conservatisms would have been an upgrading of the then-current state of the art and in a sense 'unfair' since one should not expect any particular PSA study to advance the state of the art (even though this has always been true: each major new PSA is an advance).

Some of the technical areas covered in the peer reviewers' report will be discussed here to provide an idea of the level of detail, the type of issues raised, and their resolution. The issues to be covered are:

- internal flooding sequences, concern for which arose out of the review of accident sequences, event trees, fault trees, and system descriptions;

- core-concrete interactions and vessel melt-through phenomena, concern for which arose out of the broader review of phenomena that take place during and after core-melting;

- likelihood of failure to scram on demand, concern for which arose out of review of the ATWS analysis, which the PSA had identified as a key possible contributor to overall risk.

6.1 Review of the System Analysis Work - Internal Flooding Accident

Initiating Events: The following types of initiating events were considered in the draft SNPS PSA:

- transient events incuding ATWS

- LOCAs

- Special internal events:
  - internal flood at elevation 8 in the reactor building;
  - loss of a DC bus.

The following transient events were considered:

- turbine trip

- main steam isolation valve (MSIV) closure

- loss of condenser

- loss of feedwater

- loss of offsite power (LOSP)

- inadvertent open relief valve (IORV)

- control rod withdrawal

- manual shutdowns.

LOCAs that were considered included:

- breach of the RPV larger than ECCS capacity
- large LOCA, greater than 4" in diameter
- medium LOCA, greater than 1" and less than 4" in diameter
- small LOCA, less than 1" in diameter.

For interfacing LOCAs and the internal flood analysis, initiating event fault trees were constructed in the draft PSA. Initiating event fault trees define combinations of basic events in the fault tree which lead to the occurrence of the initiating event.

It is important to note that in the analysis of initiating event fault trees, the basic event which functions as the initiating event must be identified in order that the proper units of frequency be computed for the initiating event defined by the top event. For example, consider an example of an interfacing LOCA which is caused by a non-simultaneous failure of two check valves which are in series. The top event we wish to consider is discharge from the high pressure side to the low pressure side. For this top event, the check valve which fails first is the enabling event and the check valve which fails second is the initiating event since it is the event which causes discharge from the high pressure to the low pressure side. Note that for this example, there are two time orderings that must be considered. See the case study entitled The importance of Systems and Components and Nuclear Power Plants, [ref 6], for a detailed description of the use of initiating and enabling events in PSA. In addition, see the PRA Procedures Guide, [ref 5], for a discussion of initiating-event fault trees.

As described below, an error in the draft PSA occurred in computing the frequency of internal flooding at SNPS because the units for the initiating event, which caused internal flooding, were computed in terms of unavailability instead of frequency. The authors observe that this error is common in PSA.

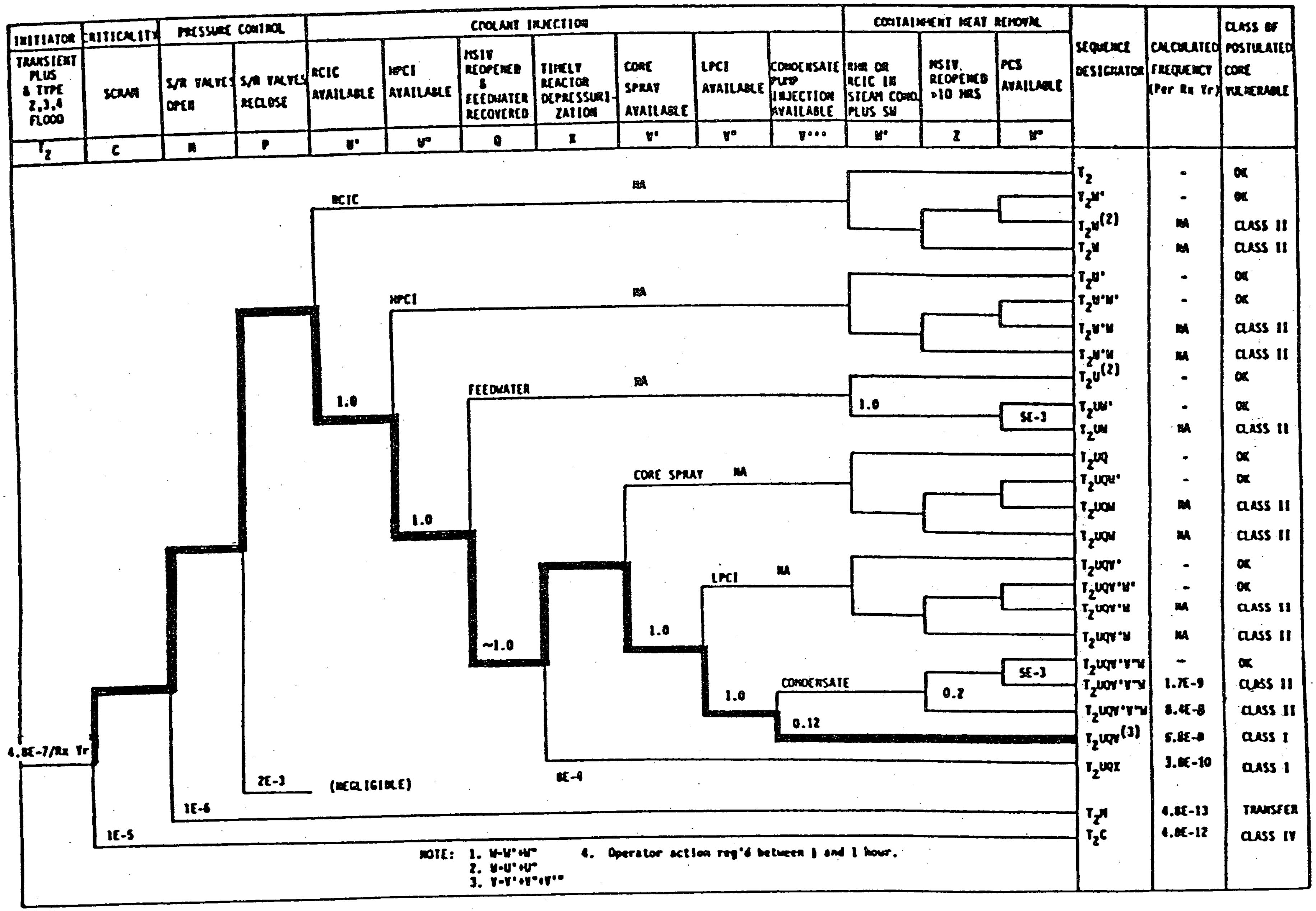

FIG. 1. Event tree diagram for sequences following a release of water into elevation 8 of types 2, 3 and 4 initiators [ref 1].

Internal Flood Analysis

We now discuss the internal flood analysis conducted in the SNPS PSA. We discuss the analysis in three steps:

- The PSA contractor's analysis of internal floods in the draft report
- the peer review of the internal flood analysis
- the PSA contractor's reply to the peer review.

It is important to note that the peer review was based upon the information given in the draft PSA. In their reply, the PSA contractor revised information regarding plant behaviour given in the draft report and provided additional information which altered some of the conclusions in the peer review.

System Description (as provided in the draft PSA)

The Shoreham Reactor Building surrounds the Mark II containment structure. At its lowest elevation (referred to as Elevation 8), the building is an open cylindrical compartment: i.e., there are no barriers in the elevation 8 compartment which would interfere with personnel access or room ventilation. However, this open area presents the possibility of adversely affecting the equipment in Elevation 8, if excessive water were released into the compartment.

In the draft report, the PSA contractor identified nine possible water sources (defined as initiator types) that could release water into elevation 8 of the Reactor Building, greater than the sump capacity. Several ECCS and residual heat removal components are located at elevation 8. In particular, the PSA contractor identified 3 initiator types, 2, 3, and 4 as described below which could quickly (within 30 to 40 minutes) flood and disable the components described in the PSA contractor's Table G.6 (Table 1 of this report) if the operator fails to reclose the isolation valve in time.

Table 1. Initiators and Vulnerable Components

Initiator	Water Source	Systems Involved
2	Containment Storage Tank	High Pressure Core Injection System (HPCI), Reactor Core Isolation System (RCIC), and Containment Spray (CS)
3 & 4	Screenwell	Reactor Building Closed Loop Water System (RBCLWS), and the Residual Heat Removal System, (RHR).

While the flooding occurs, if the operator erroneously isolates the power conversion system (contrary to normal operating procedures), then the accident sequence is initiated as described by the bold line on the event tree in Figure 1.

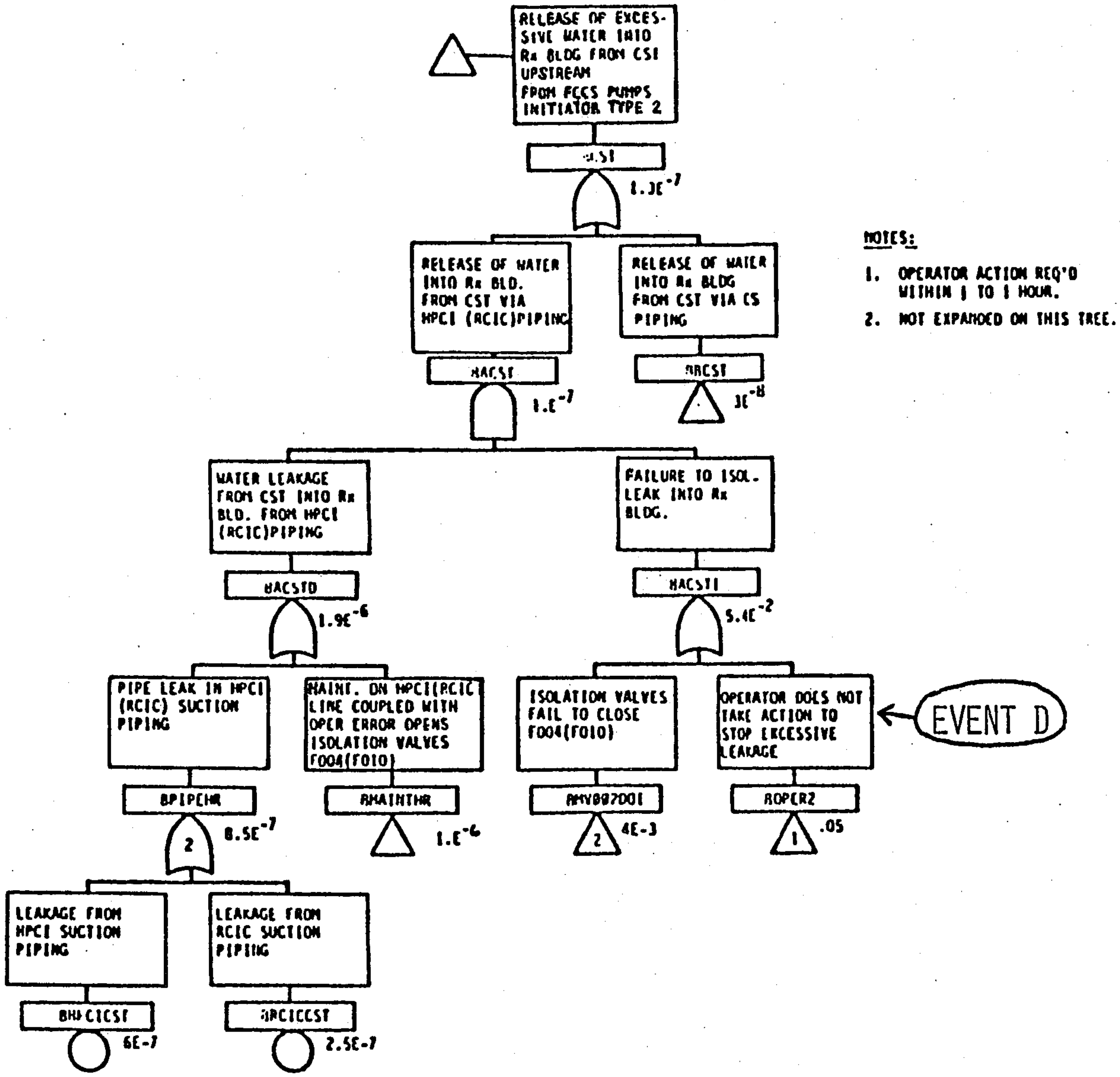

FIG. 2. A typical fault tree development for elevation B flood initiator type 2 [ref 1].

The PSA Contractor developed initiating-event fault trees which describe the following sequence of events involving operator error that lead to flooding at elevation 8 concurrent with loss of the power conversion system.

- Event A: On-line maintenance of any of the following systems occurs: HPCI; RCIC; Core Spray; RBCLCW Heat Exchanger; RHR Heat Exchanger.
- Event B: System is disassembled for maintenance.
- Event C: Operator inadvertently opens an isolation valve during maintenance causing flooding to start.
- Event D: Operator fails to reclose the isolation valve within 40 minutes which results in flooding to the six foot level.
- Event E: Operator erroneously isolates the power conversion system during flooding.

A typical fault tree development for the sequence described above is shown in Figure 2. It must be noted that the PSA Contractor combined events A and B on the fault tree.

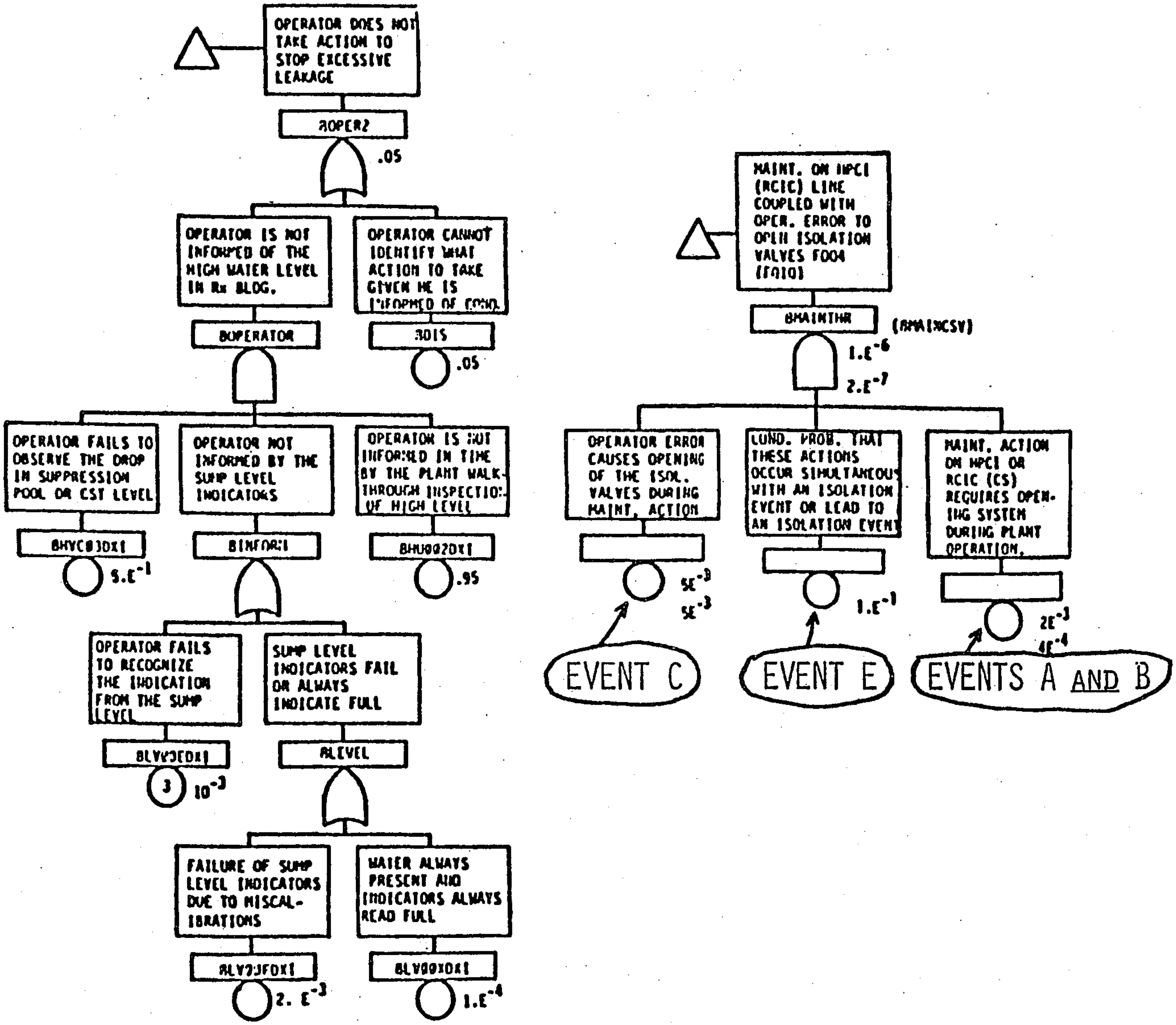

FIG. 2. (cont.)

Issues Raised by the Peer Review

Two conclusions reached by the peer reviewers are as follows:

- The approach used by the PSA Contractor in quantification of these sequences does not produce units with accident frequency. One key event in the flooding sequence is the operator inadvertently opening a valve during maintenance. The probability estimate for this event is given on a per maintenance act basis. The PSA Contractor's calculations did not reflect this, which leads to a factor of about 100 in underestimating the internal flood frequencey.

- The PSA Contractor used human probability estimates from Swain and Guttmann's work, [ref 7], that do not reflect a highly stressful situation. The reviewers believed that a highly stressful situation does exist when internal flooding occurs and that all calculations should reflect this.

The basis of the above conclusions is discussed next.

Units of Frequency Issue

As described above, event C is the initiating event which causes flooding. The occurrence of events A and B defines a vulnerable system state that permits event C to initiate flooding when event C occurs. Furthermore, the occurrence of events A and B and C defines another vulnerable system that permits event E to initiate the accident sequence when event E occurs. Because event C is an initiating event, we must compute the frequency of occurrence of this event.

Events C and D describe operator error and the PSA Contractor used Swain and Guttmann's estimates, [ref 7], to assign probabilities to these events. Specifically for event C, the PSA Contractor on page G-38 of the draft PSA said "The conditional probability that the operator opens the isolation valve to the system while it is undergoing maintenance is determined from Swain and Guttmann. The value is determined to be 0.005 per valve operation. This error rate is higher than normal plant operator states since it has been shown that operator error under maintenance conditions may be higher than that found performing normal plant function."

Using the above probability, we must compute the number of valve operations per year to obtain accident frequency, i.e., the expected number of flooding events per reactor year. The number of valve operations relates directly to the number of maintenances performed per year since the isolation valve must be closed and reopened during maintenance.

Hence the units on event A should be the expected number of on-line maintenances per year, (i.e., frequency), not system unavailability as computed by the PSA Contractor. Computation with system unavailability results in an accident frequency about 100 times smaller than with the expected number of maintenance acts per year.

In the peer review, HPCI was used as an example. The HPCI unavailability is 0.01 (units without dimensions), and its maintenance frequency is

(0.09 acts/month) x (12 months/year) = 1.08 acts/reactor year.

The reviewers claimed that the expression for accident flood frequency above the six foot elevation concurrent with loss of the power conversion system is the product of the following terms (here the symbol * means logical intersection):

TERM	EXPRESSION	UNITS
- expected number of on-line maintenances per year	E(NA(one year))	maintenance acts/year
- probability that the system is disassembled given maintenance	P(B/A)	dimensionless
- probability that the operator opens the isolation valve during maintenance	P(C/A*B)	dimensionless

TERM	EXPRESSION	UNITS
– probability that the operator fails to reclose the isolation valve	P(D/A*B*C)	dimensionless
– probability that the operator erroneously isolates the power conversion system during flooding	P(E/A*B*C*D)	dimensionless

The reason for the above functional form is that P(C/A*B) is given on a probability of operator error per disassembly basis.

Swain and Guttmann give a best estimate of 0.005, as mentioned above, but estimate the 90% confidence level of P(C/A*B) as 0.02 per maintenance outage. Because the long maintenance outage of 3.5 days (on the average) results in several shift changes, it is conceivable that the upper bound estimate may be applicable, resulting in an estimate that would be a factor of 4 higher for the flooding frequency.

Level of Stress Issue

In addition the PSA Contractor's estimate of the probability of failing to recover, P(D/A*B*C), is 0.05 which corresponds to the non-stressful situation in figure 17-2 of Swain and Guttmann. However, if stressful conditions exist, then the estimate would be a factor 5 higher, i.e., 0.25.

Also, one can see from the event tree in Figure 1 that the PSA Contractor assigned a probability of 0.12 to failing to restore the condensate system. Considering the level of stress involved, a probability of 0.25 or higher could be a more reasonable estimate.

Observations

Examining the event tree in Figure 1, one can see that the PSA Contractor calculated a frequency of 4.8 E-7 per reactor year for flooding to the six foot level (T2 initiator) and 5.8 E-8 per reactor year for class I core vulnerable accident.

However, following the arguments given above, the estimate for the T2 initiator could be as high as 1.0 E-3 per reactor year for flooding to the six foot level and 5 E-4 per reactor year (or higher) for class I core vulnerable accident - factors of 2000 difference! These class I accident figures are for the core vulnerable states to be reached: the core melt frequency would be somewhat smaller depending on an analysis that the review team did not do.

Recommendations From the Peer Reviewers

The peer reviewers recommended that the PSA Contractor recompute the internal flood frequency considering event A be given in units of frequency. Furthermore, because the internal flooding sequence is dominated by a chain of human error events, the reviewers recommended that experts in human factors carefully analyze and recompute these accident frequencies associated with internal flooding. This recommendation applies to the entire flooding event-tree sequence involving human action, i.e.

- erroneously isolating the power conversion system during flooding
- failing to provide makeup with the condensate pumps
- failing to provide containment heat removal by opening the MSIVs within 10 hours.

Also, as described in the main body of the PSA, an important assumption made by the PSA Contractor is that flooding to the six foot level will not result in automatic closure of MSIVs. (The PSA Contractor does assume that reactor trip will occur). It is important to verify that the assumption regarding automatic MSIV closure is true -- otherwise the power conversion system is lost and the normally available makeup system is the condensate system. In this case, the accident frequency caused by flooding would increase by an additional factor of about 10 and design changes may be necessary to mitigate the effects of the internal flooding accident sequence, (e.g. elevating the ECCS pumps to a higher level).

PSA Contractor's Reply to the Peer Review

A portion of the PSA Contractor's reply to the peer review concerning internal flooding is given in Appendix B of this case study. The PSA Contractor recomputed the core melt frequency due to an internal flooding accident and estimated the fractional contribution of this accident to the total core melt frequency as 3%.

Insights Gained as the Result of PSA Contractor's Reanalysis

In the draft report, the PSA Contractor did not describe the procedure for removing power from the isolation valve by racking out the circuit breaker. Existence of such a procedure makes the likelihood of internal flooding less than the reviewers originally thought. However, there were other insights gained as the result of the PSA Contractor's reanalysis, as described in [ref 8]. If for some reason, power was not removed from the breaker, then the PSA Contractor identified another means (other than human error) in which the isolation valve could be opened, i.e., a demand to start HPCI if MSIV closure should occur during maintenance. In this case, there would be other alarms other than flooding that the operator would have to recognize and respond to. Thus, the operator error of failing to reclose the isolation valve would be higher than with just a single alarm. As the result of the PSA Contractor's reanalysis, the PSA sponsoring utility became aware of the risk potential of the flooding sequence and changed operational and maintenance procedures. For example, the utility decided to change their maintenance procedures to include an independent check to verify that power to the isolation-valve breaker has been removed.

6.2 ATWS Probability: Failure to Scram on Demand

In the course of the peer review, the review team gave careful attention to the calculations involving the so-called ATWS sequences ("anticipated transients without scram"), which comprise the group that the PSA Contractors called "Class IV sequences". This careful attention was merited because in the analysis these sequences were among the most important in their effect on offsite consequences: i.e., the releases from class IV were among the key determinants of how much offsite emergency preparedness was necessary. In the PSA Contractor analysis, these class IV sequences were associated with relatively important releases, and the sequences were calculated to occur very rapidly, with containment failure prior to core melting due to overpressure, and core melting 1.5 hours after accident initiation.

The systems analysis was reviewed, and the review team concurred in the approach taken. However, in studying the quantification the review team did not agree with the data used by the PSA Contractor. Specifically, the peer review team believed that the value used by the PSA Contractor for "failure to scram on demand" was too high. If the main control rod scram mechanism fails, back-up systems are used, including the alternate rod insertion system; the standby liquid control system to inject boron; trip of the recirculation pumps; and the operator procedures.

Unfortunately, there are no empirical data for the likelihood of the failure to scram, so calculations must be relied on. The calculations are based on data that are only partially relevant to the analysis, and a model of how the failure occurs should be used. The PSA Contractor report selected a likelihood of 3 E-5 per demand for its failure rate. It was the judgment of the review team that this value was too high, by a factor in the range of approximately 3 to 10. Specifically, the review team would have used a value in the range of 3 E-6 to 1 E-5 per demand. The basis for the review team's different opinion was a careful analysis of the existing literature on this subject, which had been an important area of controversy for several years in the reactor safety community (and which remains controversial today).

In conversation with the PSA Contractor analysts, reviewers learned that the value that the PSA Contractor selected was "conservatively chosen", which is also implied in the text of the draft of the PSA Contractor report.

The impact of this judgment on scram failure is significant for the group of Class IV accidents, which would be correspondingly less likely if the value for scram failure were smaller. Because the Class IV sequences are among the most important in contributing to the need for offsite emergency response, this would affect the advice given to review sponsoring body during the development of their response plans.

The guidance that this example offers to those planning a peer review is the following: Sometimes there will arise a difference of professional opinion between reviewers and the original analysts that cannot be resolved based on the technical literature. When this occurs, it is often highly useful to the sponsor that this difference of opinion be brought forward, because it illuminates the extent to which there are limitations to the numerical results of the study, or its broader insights. An effective peer review will provide this illumination.

6.3 Phenomena After Meltdown: Vessel Breach, Drywell and Wetwell Pathways

In the course of the peer review, the study team gave detailed attention to the course of postulated core-meltdown accidents after the molten core would begin to fall into the bottom of the reactor pressure vessel. In the PSA Contractor analysis, the failure mechanism of the vessel was assumed to be either structural failure of the vessel wall due to elevated pressure and temperature, or melt-through of the main vessel wall if the pressure is low.

The review team took issue with these postulated failure mechanisms and proposed an alternate failure mechanism based on the reviewers' extensive experience. The reviewers supported their opinion with detailed phenomenological calculations. The reviewers also proposed an alternative analysis of the behaviour of molten material after it left the vessel.

The reviewers' quantitative analysis, which is documented in their review report, went significantly beyond the analysis in the PSA Contractor report itself. This situation is not typical of peer reviews, but was carried out because the reviewers believed that the analysis was necessary to understand the key phenomena after core meltdown. Based on this analysis, the reviewers provided an independent opinion as to the validity of the radioactive releases from these accidents. The reviewers' conclusion was that the releases presented in the PSA Contractor report were conservatively modelled, in that several of the phenomena were treated conservatively. However, the reviewers were unable to provide a quantitative estimate of the degree of conservatism.

The sponsors of the review thus had alternative analyses from which to judge the severity and likelihood of releases for these accident sequences.

The guidance that this example offers to those planning a peer review is that it may be necessary for peer reviewers to undertake significant new analysis in order to provide an independent opinion as to the validity of the work under review. (In the case under consideration, this involved writing a computer code by the reviewers.) If a peer review team discovers that this effort is necessary, the sponsor of the peer review may find that the proposed reanalysis is beyond the contemplated scope or the budgeted funds. This situation may not happen with every review, but it can happen. Sponsors of peer reviews must face the situation squarely when it does occur.

Appendix A

GENERAL REVIEW CHARACTERISTICS*

The following section describes the general aspects of a PRA which should be examined in this phase and the features that should be looked for. As already indicated above, neither the PRA nor the review will necessarily encompass all the items noted because of the particular circumstances of the PRA and the review.

The major aspects of the PRA which must be explored are

- the purpose;
- the major assumptions;
- the analyses;
- the results; and
- the interpretation and application.

More specifically the review should explore the following factors:

(i) the objectives of the PRA and their relation to the review objectives;

(ii) the management aspects of the PRA, emphasizing the synthesis of the PRA team, and the programmatic and technical management;

(iii) the general plant description and the associated generic and plant specific data used;

(iv) the underlying (technical) methods used in carrying out the PRA;

(v) the actual analyses involved and the associated numerical techniques applied to obtain the quantitative results;

(vi) the major assumptions in the analyses and quantifications, such as specially identified initiators, failure sequences, success criteria, systems components, level of resolution in the analysis, and operations (including human) (cf. NUREG/CR-2815 for more detailed lists);

(vii) the most prominent results in the light of the objectives ((i) above) and the guiding conditions ((vi) above);

(viii) any new, unusual, or anomalous data, methods, or results which appear in the PRA (and possibly also the absence of any such);

(ix) the interpretation made of the results in the light of the objectives and guiding conditions cited above, with special reference to systems, functional, and operational interactions, as well as to internal dependences which may impinge on overall plant safety and thus require further, more detailed analyses.

The general criteria which should govern the review are the following:

- organization and format,
- clarity,
- scrutability,

(*) Reproduced from NUREG/CR-3485, PRA Review Manual [ref 3]

- completeness,
- consistency,
- validity,
- robustness,
- reproducibility,
- utility, and
- comparability.

The general review process may be summarized (somewhat informally) in terms of a number of questions addressed to the PRA:

1. Are the inputs, methods and outputs clearly defined, appropriately chosen, and understandably reported, and do they correspond to the PRA's stated objectives?

2. Are there gaps in the data, methods, etc. in relation to:

   (a) the PRA's objectives;
   (b) available information and techniques; and
   (c) the level of detail and comprehensiveness characteristic of, for example, the Indian Point Probabilistic Safety Study?

3. Are the data used consistent with individual and general plant experience, and are anomalous data properly justified (and explained)?

4. Do the results seem to be robust in relation to uncertainties and variations in the data and methods, and, if not, is this lack of robustness accounted for?

5. Are the PRA and its results in a form which can be reasonably compared with other PRAs (despite the variations in uniformity), and, if so, can any differences be explained in terms of systems, functional and operational variations, or do they result from the analytic assumptions made, or the methodology adopted and the data used in the study?

Appendix B

RESPONSE OF PSA CONTRACTOR TO PEER REVIEW COMMENTS CONCERNING INTERNAL FLOODING DUE TO MAINTENANCE ACTS

In response to the Future Resources Associates (FRA) comments concerning the internal flood analysis appearing in the Shoreham draft PRA, a complete reanalysis has been performed. This conservative analysis estimates that there are maintenance induced internal flooding sequences involving Elevation 8 of the reactor building having a core vulnerable frequency value of 1.5E-6. This result indicates that these flooding scenarios have a small contribution to risk on the order of 3%. The following discussion compares the results of this reanalysis reconstructed according to the form of the sequence mentioned in the FRA draft report.

The FRA report presents the following approximation for a maintenance-induced-flood core vulnerable accident.

TERM	EXPRESSION
— expected no. of one-line maintenances per year	E(NA(one year))
— probability that the system is disassembled given maintenance	P(B/A)
— probability that the operator opens the isolation valve during maintenance	P(C/A*B)
— probability that the operator fails to reclose the isolation valve	P(D/A*B*C)
— probability that the operator erroneously isolates the power conversion system during flooding	P(E/A*B*C*D)

The following discussion compares the PSA Contractor's reanalysis of this expression with the analysis appearing in the FRA submittal for human error during an HPCI maintenance event.

E(NA(one year)) x P(B/A)

The FRA analysis for this combination of events was done by assuming the number of maintenance acts per year is 1.08, and the probability that a maintenance act will cause a system to be disassembled is 0.1. This yields a probability for the combination of the frequency of E(NA(one year)) x P(B/A) to be 0.108 per reactor year.

In a more detailed analysis, the PSA Contractor has used the LER data base for turbine driven pumps used in BWRs, to determine the expected number of failures per year for the pump. While all the reported failures do not require the system to be opened for maintenance, use of this number will, to some extent, account for unreported maintenance acts that cause the system to be opened.

This calculation is described in the revised Appendix A of the submittal [ref 8] and estimates the value for E(NA(one year)) x P(B/A) of 0.079. Although this number is not significantly different from the FRA value, the estimate derived from the LER data base is judged to be more realistic.

P(C/A*B)

The FRA analysis uses the upper bound of 2.0E-2/maintenance outage as the value for P(C/A*B). This value was taken from Swain and Guttmann as an upper bound due to an assumed 3.5 day maintenance outage. This value is for a simple valving error during a maintenance act.

The PSA Contractor has performed a detailed human reliability analysis of the maintenance procedure requiring isolation of the pump, the associated valves and their controls. This analysis indicates that the maintenance procedures call for power to be removed from the valve operators. When power is removed, remote operation of the valves is not possible. In addition, the location of the valves, close to the location where water would be released, makes it highly unlikely that local manual operation of the valves could take place without the operator noticing the water flow and reclosing the valve. Therefore, if power is removed from the isolation valves, it is highly unlikely that the system will become unisolated.

The probability of an inadvertent opening of an isolation valve is the product of two parts: 1) the probability that power is not removed from the valve and 2) the operator inadvertently operates the valve. The conservative estimate for the first event is 0.01, while the estimate used for the second event is 0.02. This yields a probability for P(C/A) of 2 E-4 (0.01 x0.02).

P(D/A*B*C)

The FRA analysis used the curve estimating human performance after a large LOCA to estimate the probability. The estimate used for this event by FRA is 0.25 due to the assumed highly stressful conditions.

The PSA Contractor has performed a detailed analysis of this event including a procedural and a control room review. This analysis used new information concerning cognitive behavior, and simulator data to derive a time-dependent model of operator actions subsequent to a flood event. For the event analyzed here the estimated time available for operator action is 13-17 minutes, depending on the source of water. Using this, the estimated probability for event P(D/A*B*C) is 0.1 since it is likely that the flood would be the only "off normal" event going on in the control room for an operator error induced flood during major maintenance.

P(E/A*B*C*D)

The FRA analysis of this event concludes that due to the stressful situation a value of 0.25 or higher is appropriate. In the detailed analysis, PSA Contractor has evaluated all possible dependencies that would preclude the use of the PCS (feedwater and condensate) to become unavailable during a flood event occurring while the reactor is at power. The availability of feedwater pumps was found to be dependent on operator actions following a flood event. The condensate system was found to be a highly reliable source of water in all sequences. The PSA Contractor analysis estimates the conditional probability that, given a flood, the probability of core vulnerable sequence is approximately 0.038.

EVALUATION OF THE RESULTING EXPRESSIONS

Evaluation of the expression for flood frequency is shown below:

FRA analysis:
0.108 x 0.02 x 0.25 . 0.25 = 1.35 E-4/reactor year

PSA Contractor's detailed reanalysis:
0.079 x 2 E-4 x 0.1 x 0.038 = 6.6 E-8/reactor year

The PSA Contractor believes that the detailed analysis performed shows that the core vulnerable frequency of flooding scenarios involving HPCI maintenance is conservative. A more realistic analysis estimates a frequency, 3 orders of magnitude lower than the FRA approximation found in their draft report.

REFERENCES

[1] SCIENCE APPLICATIONS, INC. (SAN JOSE, CALIFORNIA), "Probabilistic Risk Assessment, Shoreham Nuclear Power Station, Long Island Lighting Company", Preliminary Draft Report, SAI-001-SJ, March 1982.

[2] BUDNITZ, R.J., DAVIS, P.R., FABIC, S., LAMBERT, H.E., "Review and Critique of Previous Probabilistic Accident Assessments for the Shoreham Nuclear Power Station", Future Resources Associates, Inc., Berkeley, California, September 1982.

[3] EL-BASSONI, A., CHO, N.Z., HANAN, H., McCANN, JR.M.W., O'BRIEN, J., PAPAZOGLOU, I.A.' REED, J.W., SHIU, K.K., TEICHMANN, J., YOUNGBLOOD, R.W., "PRA Review Manual", NUREG/CR-3485, BNL-NUREG-51710, Brookhaven National Laboratory, September 1985.

[4] PARKINSON, W.J., VON HERRMANN, J.L., MAYS, S.E., BRINSFIELD, W.A., McCLYMONT, A.S., "An Intensive Peer Review for Probabilistic Risk Assessment, A Tool for Project Management and Staff", Report NSAC-67, Nuclear Safety Analysis Center of EPRI, Palo Alto, California, March 1984.

[5] AMERICAN NUCLEAR SOCIETY AND THE INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS, "PRA Procedures Guide", NUREG/CR-2300, January 1983.

[6] LAMBERT, H.E., MARTORE, J., HOBBS, S., "The Importance of Systems and Components at Nuclear Power Plants: Methodology and Use", IAEA TECDOC (To be published), IAEA, Vienna (1989).

[7] SWAIN, A.D., GUTTMANN, H.E., "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications", NUREG/CR-1278, April 1980.

[8] SCIENCE APPLICATIONS, INC. (PALO ALTO, CALIFORNIA), "Event Tree Evaluation of Sequences Following a Release of Excessive Water in Elevation 8 of the Shoreham Reactor Building Due to Postualted Errors During Maintenance", Report SAI-336-82-PA, November 1982.

[9] FINLAYSON, F.C., JOHNSON, J.H., FINLAYSON, F.C. AND ASSOCIATES, "A Basis for Selection of the Emergency Planning Zones for the Shoreham Nuclear Power Plant", Cerritos, California, October 1982.