NUREG/CP-0124

Proceedings of the

Workshop on the Use of PRA Methodology for the Analysis of Reactor Events and Operational Data

Held at
Loew's Hotel
Annapolis, Maryland
January 29–30, 1992

Sponsored by
U.S. Nuclear Regulatory Commission

Available from

Superintendent of Documents
U.S. Government Printing Office
P.O. Box 37082
Washington D.C. 20013-7082

and

National Technical Information Service
Springfield , VA 22161

NUREG/CP-0124

Proceedings of the

Workshop on the Use of PRA Methodology for the Analysis of Reactor Events and Operational Data

Held at
Loew's Hotel
Annapolis, Maryland
January 29-30, 1992

Manuscript Completed: July 1992
Date Published: June 1992

Sponsored by
Division of Safety Programs
Office for Analysis and Evaluation of Operational Data
U.S. Nuclear Regulatory Commission
Washington, DC 20555

EXECUTIVE SUMMARY

A workshop entitled "The Use of PRA Methodology for the Analysis of Reactor Events and Operational Data" was held on January 29-30, 1992 in Annapolis, Maryland. Over 50 participants from the NRC, its contractors, and others participated in the meetings. During the first day, presentations were made by invited speakers to discuss issues in relevant topics. On the second day, discussion groups were held to focus on three areas: (1) risk significance of operational events, (2) industry risk profile and generic concerns, and (3) risk monitoring and risk-based performance indicators.

Important considerations identified from the workshop are the following:

- Improve the Accident Sequence Precursor models and data.
- Improve the SCSS and NPRDS (e.g., by adding detailed performance information on selected components, by improving narratives on failure causes).
- Develop risk-based performance indicators.
- Use risk insights to help focus trending and performance analyses of components, systems, initiators, and sequences.
- Improve the statistical quality of trending and performance analyses.
- Flag implications of special conditions (e.g., external events, containment performance) during data studies.
- Trend common cause and human performance using appropriate models to obtain a better understanding of the impact and causes of failure.
- Develop a method for producing an industry risk profile.

CONTENTS

EXECUTIVE SUMMARY iii

ACKNOWLEDGMENTS viii

LIST OF ACRONYMS ix

1. INTRODUCTION 1

2. SUMMARY OF PRESENTATIONS 3

2.1 Accident Sequence Precursor Program Methods - Joseph W. Minarick 3

2.2 Methods for Identifying Risk Significant Trends - Gareth W. Parry 5

2.3 Approaches for Analyzing Data to Address Generic Issues Related to Common Cause Failures, Human Factors, and Systems Interactions - Ali Mosleh 6

2.4 Industry Risk Profiles: Do We Need More Modeling? - George Apostolakis 8

2.5 Use of PRAs and IPEs for Event Risk Analysis - Arthur C. Payne, Jr. 9

2.6 Living PRA Concept - Dennis Bley 11

2.7 Trending Plant Performance: Thoughts on Risk-Based Performance Indicators - Joseph R. Fragola 12

3. DISCUSSION GROUP 1 - RISK SIGNIFICANCE OF OPERATIONAL EVENTS 15

3.1 Summary of Discussion Group 1 15

3.2 Details of Discussion Group 1 16

4. DISCUSSION GROUP 2 - INDUSTRY RISK PROFILE AND GENERIC CONCERNS 21

4.1 Summary of Discussion Group 2 21

4.2 Details of Discussion Group 2 22

5. DISCUSSION GROUP 3 - RISK MONITORING AND RISK-BASED PERFORMANCE INDICATORS 27

5.1 Summary of Discussion Group 3 27

5.2 Details of Discussion Group 3 28

6. OVERALL INSIGHTS 31

7. REFERENCES 33

Appendix A - List of Workshop Attendees 35

Appendix B - Summary Paper 41

Appendix C - Discussion Group 1 Questions and Participants 55

Appendix D - Discussion Group 2 Questions and Participants 59

Appendix E - Discussion Group 3 Questions and Participants 63

Appendix F - View Graphs for "Accident Sequence Precursor Program Methods" - Joseph W. Minarick 67

Appendix G - View Graphs for "Methods for Identifying Risk Significant Trends" - Gareth W. Parry 79

Appendix H - View Graphs for " Approaches for Analyzing Data to Address Generic Issues Related to Common Cause Failures, Human Factors and Systems Interactions - Ali Mosleh 87

Appendix I - View Graphs for "Industry Risk Profiles: Do We Need More Modeling?" - George Apostolakis 95

Appendix J - View Graphs for "Use of PRAs and IPEs for Event Risk Analysis - Arthur C. Payne, Jr. 105

Appendix K - View Graphs for "Living PRA Concept" - Dennis Bley 113

Appendix L - View Graphs for "Trending Plant Performance: Thoughts on Risk-Based Performance Indicators" - Joseph R. Fragola 123

ACKNOWLEDGMENTS

Patrick Baranowsky, NRC, Dale Rasmuson, NRC, and Susan Dingman, Sandia National Laboratories, organized the workshop. Gratitude is extended to the speakers and the discussion group moderators (Allen Camp, Gareth Parry, Ali Mosleh, and Joe Fragola) for their time and effort in making the discussion sessions so productive. Special thanks are also extended to those individuals who took notes of the discussion sessions. Their efforts helped make the preparation of this report easier.

Susan Dingman prepared a draft of this report from the notes and tapes of the discussion sessions. Dale Rasmuson and Susan prepared the final report. Speakers provided written summaries of their presentations.

LIST OF ACRONYMS

ACRS	Advisory Committee on Reactor Safeguards
AEOD	Office for the Analysis and Evaluation of Operational Data
ASEP	Accident Sequence Evaluation Program
ASP	Accident Sequence Precursor
BNL	Brookhaven National Laboratory
BWR	Boiling Water Reactor
CCF	Common Cause Failure
CUSUM	Cumulative Summation Method
50.72	Immediate notification of reportable events to the NRC by licensees
FRA	Future Resources Associates, Inc.
HRA	Human Reliability Analysis
INEL	Idaho National Engineering Laboratory
INPO	Institute for Nuclear Power Operations
IPE	Individual Plant Examination
IPEEE	Individual Plant Examination for External Events
JBFA	JBF Associates, Inc.
LANL	Los Alamos National Laboratory
LER	Licensee Event Report
NPRDS	Nuclear Plant Reliability Data System
NRR	Office of Nuclear Reactor Regulation
NUS	Halliburton NUS Environmental Corporation
ORNL	Oak Ridge National Laboratory
PI	Performance Indicator
PLG	PLG, Inc.
PRA	Probabilistic Risk Assessment
RES	Office of Nuclear Regulatory Research
SAIC	Science Applications International Corporation
SCSS	Sequence Coding and Search System
SNL	Sandia National Laboratories

1. INTRODUCTION

Operational data from a variety of sources are reviewed and evaluated by NRC to identify 1) significant events and any associated safety concerns and root causes, 2) the trends and patterns displayed by these events, 3) the adequacy of the corrective actions taken to address these concerns, and 4) the generic applicability of events and concerns to other plants. Although programs are in place to perform these evaluations, it is recognized that there are shortcomings in the processes currently used.

A workshop was held in Annapolis, Maryland, on January 29 and 30, 1992, to discuss the current methods and the potential for their improvement. The objective of the workshop was to exchange technical information on enhancing the use of PRA methods, information, and insights in NRC's analyses and evaluations of operating reactor experience. Over 50 participants attended the workshop. A list of attendees is included in Appendix A. The workshop was directed at the following topics:

(1) Use of existing PRAs and IPE models and results in performing routine event evaluations (rapid/quick-look assessments and enhancements to ASP models and methods).

(2) Methods and approaches for evaluating industry risk profiles (trends).

(3) Innovative uses of existing/available data sources (LERs, 50.72s, NPRDS, other untapped data sources) to identify risk significant trends and safety issues.

(4) Potential new plant-specific risk-based performance indicators (direct and indirect (surrogates), data needs and availability).

(5) Risk-based approaches to selecting and analyzing plant-specific and "generic" trends and patterns, including common cause failure, systems interactions, and human performance concerns.

(6) Analytic methods, software, and/or procedures which could be used, adapted modified, improved, or developed to enhance operational data analysis.

The workshop was conducted to explore methods and approaches that could provide the ability to focus on risk relevant concerns more quickly and provide a more thorough culling of operating reactor experience data than techniques currently available and in routine use at the NRC.

A paper summarizing the NRC's recent and current programs and activities related to operating reactor events/data analysis was provided to each participant prior to the workshop. That paper is found in Appendix B. Seven invited speakers were asked to

address selected issues related to the workshop objective. Summaries of their presentations are found in Section 2.

The first day was dedicated to introduction and presentations by the initial speakers. On the second day, the participants divided into three smaller groups to exchange ideas. Each group was assigned a general topic for major consideration. The discussion groups focused on 1) the risk significance of operational events, 2) evaluating an industry risk profile and the consideration of the generic implications of events, and 3) methods for monitoring risk and developing risk-based performance indicators. Each discussion group was furnished a set of questions for consideration (listed in Appendices C, D, and E). The groups were also encouraged to deviate from the list if they felt it to be appropriate. Following the discussion sessions, a summary and wrap-up session was held where the discussion group moderators presented highlights of their sessions.

The workshop discussions are summarized in Sections 3, 4, and 5 of this report. Each section consists of two subsections. The first is a summary of the discussion group findings, and the second contains more detailed information from the group discussions. The ideas summarized in this report were not necessarily shared by all participants. Meaningful ideas expressed by individuals are contained in the report, even though others in the discussion groups might not have agreed with the concept or its perceived importance. Section 6 contains a summary of the important insights obtained from the workshop.

2. SUMMARY OF PRESENTATIONS

Seven speakers were invited to address selected issues related to the workshop objective.

The titles of the presentations and the speakers are:

(1) Accident Sequence Precursor Program Methods - Joseph W. Minarick,

(2) Methods for Identifying Risk Significant Trends - Gareth W. Parry,

(3) Approaches for Analyzing Data to Address Generic Issues Related to Common Cause Failures, Human Factors, and Systems Interactions - Ali Mosleh,

(4) Industry Risk Profiles: Do We Need More Modeling? - George Apostolakis,

(5) Use of PRAs and IPEs for Event Risk Analysis - Arthur C. Payne, Jr.,

(6) Living PRA Concept - Dennis Bley, and

(7) Trending Plant Performance: Thoughts on Risk-Based Performance Indicators - Joseph R. Fragola.

Summaries of these presentations, based on summaries furnished by the speakers, are given in this section.

2.1 Accident Sequence Precursor Program Methods, Joseph W. Minarick[1]

Accident sequence precursors are operational events that are important elements in severe core damage accident sequences. Such precursors can be infrequent initiating events or equipment failures that, when coupled with one or more postulated events, could result in a reactor plant condition leading to severe core damage. The NRC's Accident Sequence Precursor (ASP) program searches operational events for such precursors, analyzes and ranks them as to their likelihood of proceeding to core damage, and identifies important sequences that, more likely than others, could lead to severe core damage.

Events are currently selected and documented as accident sequence precursors if they include a core damage initiator requiring safety system response, or the failure of a system or degradation in more than one system required to mitigate the consequences of a core damage initiator, and if the conditional probability of proceeding to core damage is estimated to be at least 10^{-6}. Events not addressed due to low significance and

[1]Appendix F contains the view graphs for this presentation.

programmatic constraints include uncomplicated reactor trips, losses of feedwater without additional failures, single failures in mitigating systems, and design errors discovered by reanalysis. With the exception of initiating events, precursors typically involve events not considered when applying the single failure criterion used in the design of safety-related systems.

Precursors are quantified primarily for ranking purposes - to identify events which may deserve additional scrutiny. Quantification involves determination of a conditional probability of subsequent severe core damage given the failures observed during an operational event. This is estimated by mapping observed failures onto event trees depicting potential paths to severe core damage, and calculating a conditional probability of the event through the use of branch probability estimates modified to reflect the event. The conditional probability estimated for each precursor is useful in ranking events because it permits estimation of the measure of protection against core damage remaining once the observed failures have occurred.

The event sequence models used to rank precursors as to significance consist of plant-class specific event trees and simplified plant-specific system models. These models describe mitigation sequences for three initiating events: a nonspecific reactor trip (which includes loss of feedwater within the model), loss of offsite power and small-break LOCA. The event sequence models are system-based and include a model applicable to seven plant classes - three for BWRs and four for PWRs.

The potential for recovery is addressed in the precursor analyses by assigning a recovery step to each failure and initiating event. This assignment is based on engineering judgment, which considers the specifics of each operational event and the likelihood of not recovering from the observed failure in a moderate to high-stress situation following an initiating event. For analysis purposes, consistent probabilities of failing to recover an observed failure are assigned to each event in a particular recovery class. Four recovery classes, based primarily on the location where recovery actions would be required and the extent that such actions are proceduralized, are currently used to describe the different types of recovery that could be involved.

The quantification process for each event involves a determination on initiators which must be modeled and their probability, plus any modifications to system probabilities necessitated by failures observed in an operational event. Once the branch probabilities that reflect the conditions of the precursor are established, the sequences leading to the modeled end states (core damage and ATWS) are calculated and summed to produce an estimate of the conditional probability of each end state for the precursor. So that only the additional contribution to risk (incremental risk) associated with a precursor is calculated, conditional probabilities for precursors associated with equipment unavailabilities (during which no initiating event occurred) are calculated a second time using the same initiating event probability, but with all branches assigned normal failure probabilities (no failed or degraded states), and subtracted from the initially calculated values. This eliminates the

contribution for sequences not impacted by the precursor, plus the normal risk contribution for impacted sequences during the unavailability.

In the quantification, it is assumed that the failure probabilities for systems observed failed during an event are equal to the likelihood of not recovering from the failure or fault that actually occurred. Failure probabilities for systems observed degraded during an operational event are assumed equal to the conditional probability that the system would fail (given that it was observed degraded) and the probability that it would not be recovered within the required time period. The failure probabilities associated with observed successes and with systems unchallenged during the actual occurrence are assumed equal to a failure probability estimated from either system failure data (when available) or by the use of system success criteria and typical train and common-mode failure probabilities.

Operational events which satisfy the precursor selection criteria are documented annually (NUREG/CR-4674 series reports [1]). While the selection of precursors has remained relatively consistent over the 1984-90 observation period, some differences do exist in those which have been documented. These differences relate to the types of events selected, the accident sequence models utilized, and the application of a minimum conditional probability (10^{-6}) before an operational event is documented (for 1987 and later). These inconsistencies must be considered when comparing the numbers and types of events in different time periods.

Improved event tree models are being developed for use in evaluation of daily events by NRR. These models are based on the ASP models, but reflect NUREG-1150 insights to a greater degree than the current ASP models, include additional initiating events, and address alternate long-term cooling strategies. These models will be usable in the ASP program once they are completed.

2.2 Methods for Identifying Risk Significant Trends - Gareth W. Parry[2]

The topics discussed during this presentation included: (1) methods to screen event data for risk significance, (2) analysis of the reduced data for trends, and (3) data needs for meaningful analysis.

The talk addressed the use of PRAs to help identify trends in data provided by event data bases such as the LERs, and component data bases such as NPRDS. One important role of a PRA was identified as being a filter to screen for risk important events using the tools of importance analysis. However, PRAs have limitations. They generally do not model non-full power states, they do not include all components, and they do not model failure causes. In addition, there may be important assumptions which impact the structure of the model,

[2]Appendix G contains the view graphs for this presentation.

and thereby the assessment of importance of certain events. Nevertheless, with care, a PRA can be a very useful tool.

An important issue is how to perform screening. Should events be assessed against all plants or just at the plant in which they occurred? The reason for assessing events against all plants is that events, which do not cause significant problems at the plant where they occurred, may indicate potential problems at others. Also, degraded states, as opposed to failures, when analyzed for their causes, may indicate trends or underlying problems. Analyzing events in this fashion would increase the work considerably, and also means an analyst must understand a lot about the events. This is probably not very practical, although this is probably where the biggest value may lie. Essentially one would have to have a "model" of the event that addresses the whole chain of sub-events that lead to the event. This was illustrated by reference to the cause-defense approach to the analysis of CCFs [Reference 2]. (This would be in the nature of an ideal case.)

Given a set of screened data has been obtained, there are many methods to analyze for trends. The methods themselves were not discussed in any detail. However, it was pointed out that this cannot be done in a random fashion. The analyst has to have some idea of what he is looking for, as this will tell him how to partition the data. Therefore, it is important to establish a cause-effect hypothesis before analyzing the data. Some examples were given of how this impacts grouping of data. For example, in exploring aging, the time origin is start of life, whereas in exploring the impact of regulatory changes, the origin should be taken as the date of implementation. Since the models are to be used to identify trends, they do not need to be mathematically structured, a qualitative understanding of the effect of changing the independent variable may be adequate.

Establishing these cause-effect models also helps understand what, if anything, is missing from the data as it is currently collected that prevents the hypothesis/models being tested correctly. An example was given of the data needs that have been established for common cause failure analysis [2].

2.3 Approaches for Analyzing Data to Address Generic Issues Related to Common Cause Failures, Human Factors, and Systems Interactions - Ali Mosleh[3]

To improve the quality of the accuracy of PRA models, operational data must be used both qualitatively and quantitatively. Equally important, but much less acknowledged, is the need for an underlying model to guide data collection and analysis. These two processes ought to be interactive and iterative, leading to an evolutionary improvement in models and data.

A common cause failure (CCF) event can be decomposed into two key elements. The failure depends on the occurrence of a trigger event (such as a flood in a particular room)

---

[3]Appendix H contains the view graphs for this presentation.

and then on a coupling mechanism which results in multiple failures (such as two pumps being located in the same room with motors susceptible to moisture). CCF events can be classified into two categories, with Type I indicating failures almost immediately after the trigger events and Type II indicating delayed failures. Each of these classes can be further divided into classes in which the coupling factor couples components in either a random or a dependent fashion.

Data needs for analysis depend on the level of the CCF model. For effective use of current models, the following are needed:

- More accurate description of the events is needed in terms of cause and impact of the event,
- Level of redundancy, and
- Success data.

Improved models will need (as a minimum) information on:

- Coupling factor(s),
- Barriers and defenses both against the cause and the coupling, and
- Failure times.

Future models will need, in addition to the above, information on the physical nature of the root cause and coupling factor of the events.

CCF events are rare. For example, a two-unit plant with more than 22 years of operational data has only experienced six CCFs, which is about 5% of all failures experienced. Out of more than 4000 LERs reviewed, only about 150 were CCFs of the type modeled in PRAs (power operation only). Review of the CCF data indicates common characteristics with generic implications, particularly with respect to coupling factors and defense strategies.

Plant-specific PRAs must consider industry (generic) experience for completeness of CCF modeling and realistic assessment of probabilities. Data from various plants need to be analyzed according to a comprehensive classification system in order to gain generic insights into the underlying causes of CCFs. Current data reporting systems (including LER and NPRDS) lack adequate recording and reporting guidelines for CCF events.

Human reliability estimates as applied to nuclear power plant PRAs are almost completely based on judgement. Even in those cases where data collection has been attempted, models which are neither validated nor supported by a theoretical or empirical foundation dominate

the results. With the exception of a recently instigated AEOD program, there has been no systematic effort to compile and analyze actual operating experience from a human performance point of view. Generally speaking, current models do not reflect actual operating experience. Even qualitative insights from the limited operational data have not been used systematically in the models.

Complete quantitative data required for calculation of error probability estimates are sparse (at least for direct estimation) since success data are very difficult to obtain. Nevertheless, some consideration should be given to identifying possible approaches for collecting success data. This might be easier in the case of operator response to initiating events. Efforts in the area of collecting, analyzing and classifying human performance data should be expanded. The direct benefit will be in gaining insights into causes and modes of human errors. Such insights can be used to improve plant safety, sometimes with minor changes in plant or operating practices and procedures. They can also provide much needed "real life" input to the human reliability model building activities.

2.4 Industry Risk Profiles: Do We Need More Modeling? - George Apostolakis[4]

The principal thesis of this presentation is that operational experience is of limited value, unless it is interpreted through validated models. However, it is recognized that developing such models may require the expenditure of significant resources. This thesis is supported by three classes of problems that can serve as illustrative examples.

The first class of problems deals with failure rates of components. Neglecting the plant-to-plant or environment-to-environment variability of the failure rate may lead to distortions of its distribution. For example, the high tail of the distribution normally reflects severe accident environments. Since most of our operational experience is from routine tests, any updating of the distribution should not affect this tail. This important point is not always appreciated and, as a result, unreasonably narrow distributions may be produced. Relevant references are [3-4]. Furthermore, the evidence itself may require interpretation and this can only happen through the appropriate models [5-6].

The second class of problems emphasizes the usefulness of reliability physics models. These require that individual models be developed for the various physical mechanisms that may lead to component or system deterioration and failure. By going down to this detail, we can include the evidence in the place where it belongs. For example, such physical models are used in the analysis of "external" events (earthquakes, fires, etc.). Thus, strengthening a structure or improving the fire resistance of cables can be accommodated at the right place in the overall methodology. Aging effects can also be considered [7].

---

[4]Appendix I contains the view graphs for this presentation.

The third class of examples deals with human actions and the factors that may influence them. A very well known incident is the one that occurred at Davis Besse on June 9, 1985 [NUREG-1154]. Part of the sequence of events was the hesitation of the shift supervisor to initiate bleed-and-feed cooling, in spite of the recommendations of the secondary-side operator and of the operations superintendent. This hesitation has been discussed widely, and people have speculated regarding its causes. For example, it is stated in NUREG-1154 that "the shift supervisor appreciated the economic consequences of initiating MU/HPI [bleed-and-feed] cooling." What is very interesting is that the precursor report NUREG-4674 treats this hesitation as a **non-event**. All kinds of recommendations are made based on events that are clearly perceived as failures (e.g., the incorrect actuation of the Steam and Feedwater Rupture Control System). However, there are no specific recommendations stemming from this observed hesitation. One could, in fact, argue that this hesitation may be an indication of senior management's priorities, in which case many different accidents may be affected. The reason for this omission is that the writers of NUREG-4674 had no model of operator behavior which allowed them to place the incident in perspective and to investigate its possible causes and/or consequences in a systematic way. The problem is, of course, that, even if they had been willing to use such a model, they would have found very quickly that it did not exist. Some preliminary thoughts are given in [8], but they are, indeed, very preliminary. This is a striking example in which the lack of a model leads us to essentially ignore an important piece of operating experience.

2.5 Use of PRAs and IPEs for Event Risk Analysis - Arthur C. Payne, Jr.[5]

Current estimates of risk from nuclear power operation are based on either PRAs or operational event analyses. Through PRAs, we identify combinations of equipment failures and human actions that lead to risk-significant events. These assessments are limited by our current understanding of aspects such as system performance, phenomena, human performance, etc. Because we are concerned that we might have missed some important aspects of plant response, we turn to operational data for potential insights. However, operating data can not indicate all potential problems because the events rarely occur. An approach is suggested here that would gain insights by comparing PRAs and operational data assessments. These insights could then be fed back into both types of analyses to yield better results.

The basic idea of the proposed system is to use expert systems to continually contrast PRAs and operational data analyses to get constant improvement in our identification and understanding of potential accident precursors. A two-fold approach is used. First, new events are examined to help identify any weaknesses in the analysis methods. Second, comparisons of operational events with known risk-significant events are made to identify those events that are important enough to merit furtner investigation. The following method is proposed:

---

[5]Appendix J contains the view graphs for this presentation.

Event Identification and Classification

1. A model of the characteristics of both PRA events and operational events is constructed. Because the approaches each have unique aspects, the characteristics would be expected to be different.

2. As new PRAs are performed and operational events are observed, the model describing the characteristics of events is reviewed for completeness, and updated if necessary. An expert system would be developed for this process. The expert system and analyst would compare the new events to the model of event characteristics and determine whether or not the current model is adequate. If not, the additional characteristics encountered with the new event are added to the model of event characteristics.

3. The system modeling and data analysis techniques are compared to the theoretical model to develop an understanding of the limitations of each technique and possibly generate improved models.

4. The expert system reviews the data base of PRA and operational events to reclassify events using any new characteristics. The expert system would identify events that might have the new characteristics for which the current information is insufficient to conclude this for sure.

Event Importance to Safety

1. A data base is constructed that consists of PRA results, data bases such as LERs, NPRDS, etc.

2. An expert system is devised that will allow the analyst to enter a description of an event (either observed through operation or identified in a PRA) and then compare the event to the characteristics of events that have previously been determined to be significant to risk. If the event characteristics do not match the characteristics of any risk-significant event, the system would identify those additional characteristics that the event would require in order to be important to risk. The system should also be able to compare the characteristics of different plant designs and be able to identify those plants at which an event might be important.

3. For the evaluation of the importance of new events, an interface with a set of PRA analysis codes such as IRRAS would be developed so that the analyst could: modify the models as appropriate, input the effect of an event into the affected models, and then evaluate the results for affected plants. The models could be surrogates at various levels of detail (current ASP, ASEP, IPE, or full PRA) or could be individual plant models, also at various levels of detail.

The level of detail should probably be at least to the level that support systems are explicitly in the model.

4. A data analysis capability would be developed so that the analyst could keep track of all identified precursor events and keep an up-to-date quantification of those events which have occurred.

2.6 Living PRA Concept - Dennis Bley[6]

The most important characteristics of a living PRA were discussed. The models and data need to reflect current plant conditions so that the PRA model will provide an accurate representation of the current status of the plant. The models need to be constructed such that the physics, system interactions and dependencies, and human interactions properly reflect the real plant. Also, to provide an accurate representation, the essential systems all need to be included in the model. To be useful, the PRA must be adaptable so that new questions can be answered. The model must be easily modifiable so that proposed plant changes (hardware, procedures, technical specifications) can be tested.

There are several uses for living PRA. Living PRA can be used to identify weaknesses in the plant, as a risk management tool, and to support the higher level overall risk/decision analysis. As a risk management tool, it can be used to set priorities for maintenance, training, and plant changes, thus optimizing fixed budget/time frame efforts. It can provide the basis for planning and developing accident management procedures and has the potential for providing real-time projections and decision support during some accidents. Living PRA can also be used as an educational tool for developing an improved risk awareness by operators and management. It can also be used to evaluate the significance of operating experience.

To be fully effective, living PRA must be understandable so that the risk implications can be communicated outside the PRA community. Examples were shown of some approaches for more effectively presenting the PRA.

There are some additional requirements for living PRA beyond those present in traditional PRAs. Configuration management of the PRA model will be a concern because the models and data will be continually updated. There will be a need for continual updates to reflect plant changes, new failure data, new models suggested by industry events, etc. In the talk, an example was presented of a structure for the PRA that was developed to simplify the task of updating the PRA. Smaller, simpler event trees were constructed for plant maintenance, configurations during various plant states, support systems, etc. The individual trees could be easily updated in this form and then linked together to give the integral result.

---

[6]Appendix K contains the view graphs for this presentation.

Advanced methodologies such as dynamic interaction models, human cognitive models, and organizational models may be appropriate. Advanced computer tools need to be implemented for improved reporting speed, query capability, and communication. Possibilities to explore include artificial intelligence, hypertext, and improved graphics tools.

Living PRA could be used as a tool for performing plant-specific examinations of precursor events and to identify weak spots in PRAs. It gives an incentive for doing cross classification of information coming out of the precursor program to support verification of human error rates, system/subsystem unavailability, etc.

2.7 Trending Plant Performance: Thoughts on Risk-Based Performance Indicators - Joseph R. Fragola[7]

Indicators of the safety performance of any plant or system provide information concerning the past, current, and/or future performance of that plant or system. Indicators can be either direct or indirect, leading or lagging. While these appellations are not exact labels, it is true that in the former set direct indicators are those provided by variables themselves or by simple evaluation of performance functions by the direct insertion of variable values. On the other hand, indirect indicators are those which correlate in a non-random fashion with plant or system performance. In this case the analytical relationship responsible for this correlation may be somewhat obscure or even totally unknown. In the latter set of labels, "leading" indicators are those which presage future performance while "lagging" or "assessment" indicators deal with a determination of the past or current performance. By their nature, lagging indicators tend also to be direct, and correspondingly, leading indicators tend to be indirect, but these general tendencies should not be considered ironclad rules.

Different types of indicators play different roles in providing information on the safety and "health" of operating commercial nuclear power plants and in detecting trends in that health. Consider the analogy to human health. In this case, if the body of a particular individual is considered analogous to the plant, and the diagnostician the NRC regulator, what insights can be drawn? Firstly, it should be recognized that no diagnostician makes a diagnosis and suggests a course of action on one indicator alone. This is only accomplished via the review of a systematic collection of indicators. The diagnostician must be well aware of the anatomical systems in the body and their naturally healthful state. When the patient exhibits acute symptoms, they are brought to the attention of the diagnostician. These he must investigate in light of his knowledge of the normal healthful state of human system and in light of this particular patient's history so that he can determine if the symptoms indicate a potentially serious condition and what actions must be taken to mitigate its development. Finally, on a regular basis, the diagnostician should review the vital signs of the patient to indicate the presence or absence of potential deviant signals. This should be done in an

[7]Appendix L contains the view graphs for this presentation.

attempt to determine which patients might need special attention to investigate their health condition further without any acute symptoms of which the patient is aware.

In the same sense, these three tools; knowledge of anatomy and specific health history, recognition of and determining the implications of acute symptoms, and recourse to regular, albeit indirect, indications of health via vital sign monitoring are the heart of any performance indication system. In the commercial nuclear power plant context, a well structured and implemented PSA or IPE can provide insight into the anatomy of the plant. When this is compared with a thorough review of the plant operational history, it provides a sound basis for the first tool in the set. However, the consequence severity and the rare occurrence nature do not allow us to limit the occurrence of acute symptoms only to an individual plant. To expand the data set, all plants must be considered as symptom generators and insight into the potential for a serious condition must necessarily be assessed somewhat generically. It is in this manner that the Accident Sequence Precursor Program (ASP) provides (to at least some degree) the second tool.

As good as these tools might be, they do not provide for the capability of having a reasonably, rapidly reacting indicator which portends the potential for individual plant performance degradation in almost real time. Any such indicator must able to act quickly, must be able to be provided in a regular fashion from an objective data set, must be reasonably correlated to plant performance, and must produce an acceptable level of false positives and negatives. One potential indicator which was considered, after a comprehensive review which investigated over several dozen possibilities, was the average daily power level at a plant. The average daily power level offers advantages in that it is recorded daily and reported monthly. It is also objective in that it could be a metered output of the plant.

The question is whether by using average daily power level and constructing indicators in terms of its variations and fluctuation could a leading indicator of plant performance be provided? Study seems to indicate, at least after initial review, that combinations of measures derived from the average daily power level signal can be of significant value in indicating future individual plant trends. If these initial results are confirmed, it appears that this measure set can be correlated with actual future plant performance in over 75% of the instances and provide validated predictions within a three to six month time frame. The use of such an indicator could be of significant value to aid in prioritizing regulatory resources, and when combined with the PSA and ASP tools represents a formidable arsenal to attack the problem of commercial nuclear power plant performance trending.

3. DISCUSSION GROUP 1 - RISK SIGNIFICANCE OF OPERATIONAL EVENTS

Discussion Group 1 focused on the risk significance of operational events associated with an individual nuclear power plant. The suggested discussion questions are found in Appendix C. Section 3.1 contains a summary of the important information and insights produced by the discussion group, and Section 3.2 contains a more detailed presentation of the information.

3.1 Summary of Discussion Group 1

This group discussed problems in evaluating the risk significance of operational events. The group primarily addressed weaknesses with current approaches, data needs for improved assessments, the role of uncertainty evaluation in operational event analysis, and general implementation concerns.

The group identified three main areas where improved modeling is needed for the ASP program: (1) developing plant-specific train level models, (2) treating degraded equipment in addition to failed equipment, and (3) improving screening methods to ensure that the important events are efficiently identified. In addition to plant-specific train-level models, it was felt that more detailed models (to the component level) should be developed as information becomes available from the IPEs. These models could be used to supplement routine ASP evaluations with more in-depth evaluations when necessary. Such models would require verification.

In terms of completeness, four potentially important areas, currently not considered in the ASP program, were identified: (1) low probability/high consequence events, (2) external event implications, (3) design and construction errors, and (4) low power/shutdown events. It was felt that these should not necessarily be analyzed for their risk significance, but flagged as potentially important.

Inadequacies in data reporting were also noted as impacting the quality and usefulness of the ASP results. The validity of the risk estimate is dependent on the quality of the information in the operational events data report. The current data reporting system was felt to be inadequate. Some specific means of upgrading the data were identified. For LERs, a description of the plant configuration at the time of the event should be included. This should also include the status of all safety or safety-related equipment (e.g., whether the equipment is operable, inoperable, or in maintenance). Other data sources besides LERs should be utilized. It was suggested that interactions be initiated with the utilities to bring the models and failure data they are developing for their IPEs, IPEEEs, etc. into a data base, if feasible.

The role of uncertainties in operational event analysis was felt to be goal dependent. For screening and ranking purposes, point estimates were generally considered adequate.

However, for quantitative use in determining risk profiles for decision making, uncertainty/sensitivity evaluations would be needed to provide a better risk profile.

Some consideration was also given to potential methods for discovering unknown problems. Such an activity would be complementary to the ASP analyses. An approach, similar to "black hatting" in sabotage analysis, was suggested in which individuals would look through the events and try to envision combinations of failures or actions that could lead to problems.

3.2 Details of Discussion Group 1

This group discussed problems in evaluating the risk significance of operational events. The group primarily addressed modeling weaknesses with current approaches, data needs for improved assessments, the role of uncertainty evaluation in operational event analysis, and general implementation concerns.

Various uses of ASP were cited throughout the discussions, and in fact, the different possibilities sometimes appeared to add confusion to the discussions when various participants were discussing ASP issues for different uses without recognizing that they were each considering different end uses. The possibilities discussed included screening events to identify those that warrant more in-depth evaluation, identifying problem areas at plants, providing estimates of plant risk conditional on the event occurring, providing data for benchmarking plant performance relative to PRA assumptions, and trending plant and/or equipment performance. During the discussion, it was generally agreed that the most appropriate use of ASP is for screening events. Subsequently, it was noted that ASP analyses normally lag the events by a significant time, so isolated events have already been identified for in-depth review before the ASP analyses are performed. ASP has been found to be most useful for identifying groups of events to analyze and as a check that the appropriate events were analyzed. NRR is also using ASP for rapid evaluations of events, with some coordination with the AEOD activities.

The appropriate risk measure to use in precursor studies was discussed. Possibilities ranged from using estimates of health risk to using the probability that the needed systems would be available to respond during the particular event. Concerns were raised regarding data availability for measures that go beyond core damage probability, but it was felt that events with containment bypass potential should be flagged.

The group discussed the need for improved ASP models and determined that the modeling quality needed depended on the particular end use of the ASP results. Three main areas where improved modeling is needed for the ASP program were identified: (1) developing plant-specific train-level models, (2) treating degraded equipment in addition to failed equipment, and (3) improving the screening methods to ensure that the important events are efficiently identified.

The IPEs were viewed as useful for developing train level models, but there was concern over using the specific models and quantification that are submitted. The IPEs were felt to be most useful for identifying system configurations. Significant effort would be required to develop such models for use in the ASP program. Another suggested use was to use the IPEs to establish plant vulnerabilities that would be textually described (vs. quantitative inclusion) for use by the ASP analyst. The IPEs might also be used to identify plant-specific recovery actions. In addition to plant-specific train level models, it was felt that more detailed models (such as component-level models) should be developed as information becomes available from the IPEs. These models could be used to supplement routine ASP evaluations with more in-depth evaluations when necessary. The IPE models would need verification, and this is not currently being done.

Methods for treating degraded equipment are not currently available for PRAs or ASP. When degraded conditions are detected without failure, the degraded equipment should probably not be modeled as failed, yet it would have a higher probability of failure than the previously assessed value. New techniques would be needed to adjust the failure rate appropriately.

The selection criteria for ASP events and the labor intensive approach currently needed for performing the reviews were discussed. Generally, multiple failure events are selected, rather than single failure type events. The possibility of further automating the process was discussed but it was felt that it was unlikely that the process could be refined much further without changes to the SCSS program. The problem of estimating generic implications of a specific failure was discussed, that is, a plant other than the plant that experienced the event might have a specific vulnerability which if coupled to the particular event could be a problem for that the plant (but not the plant at which the event actually occurred). It was suggested that plant-specific models be implemented to overcome this difficulty, and that attempts be made to involve plant personnel in the evaluation.

It was suggested that the ASP models be sent to the plants for review, and noted that this has been done in the past. The responses from the plants were typically one-sided, pointing out unavailabilities that were too high, but seldom indicating a value was too low.

In terms of completeness, four potentially important areas, currently not considered in the ASP program, were identified: (1) low probability/high consequence events, (2) external event implications, (3) design and construction errors, and (4) low power/shutdown events. It was felt that these should not necessarily be analyzed for their risk significance, but flagged as potentially important. Conditional core damage probability should be the primary ASP measure for evaluation, but other risk measures such as containment failure or health risk should not be ignored. It was felt that ASP is not the appropriate tool for evaluating these other measures, but it could be used to flag events with potentially high consequences such as containment bypass.

Events that are important, when considered with the potential occurrence of an external initiator (e.g., fire, flood, earthquake), should also be flagged. One possible way of doing this would be to identify the types of events that tend to be dominant in external event PRA accident sequences, i.e., failures that are significant in combination with external event initiators.

Design and construction errors and low power/shutdown events should also be flagged for further evaluation. Design and construction errors would be difficult to analyze in ASP because the failure to meet the design basis is identified in the LER, but the margin is not given. The utilities are generally reluctant to provide further details because the problem would normally have been fixed and no longer a concern to them. Guidance from the low power/shutdown PRAs might be needed before these events could be treated in ASP. The number of possible system configurations are significantly greater than at full power.

It was noted that support system failures with interdependencies require significant knowledge of the actual ASP coding to evaluate. The feasibility of using IRRAS/SARA to overcome these difficulties is being examined by NRR and NRC contractors. IRRAS/SARA would also allow uncertainties to be included in the evaluations. Further, importance measures would be available which could be used to identify the important equipment given a particular event has occurred (which could be different from the important equipment identified in an unconditional PRA).

Inadequacies in data reporting were also identified as impacting the quality and usefulness of the ASP results. The current data reporting system was felt to be inadequate. The validity of the risk estimate is dependent on the data quality. Some specific means of upgrading the data were identified. First, a description of the plant configuration at the time of the event should be included in the LERs. The utilities should report any other known system unavailabilities at the train level (in addition to the cause of the trip), in addition to inoperable systems. Under the current reporting requirements, the LERs are often so cryptic that they are difficult if not impossible to use. An event should not be split across LERs, as is currently done in some cases. A flag that would link LERs to the 50.72s previously called into the NRC operations center would be useful. There were felt to be other deficiencies in the LERs, but they were not specifically listed by the group.

It was noted that there might be resistance for improved reporting because it may not acceptable to impose additional reporting requirements. It was noted that the standards for LER reporting are currently being revised, but the revisions will mainly address reportable events, rather than the quality of reporting.

It was suggested that data reporting might be improved by reducing the adversarial relation between NRC and the utilities and/or giving more incentive instead of penalty for reporting events.

It was felt that other data sources should be tapped for the evaluation. The frequency of entering technical specification action statements was felt to be a good indicator of potential equipment problems. It was suggested that interactions be initiated with the utilities to bring the data they are developing for their IPEs, IPEEEs, etc. into a data base.

The role of uncertainties in operational event analysis was felt to be goal dependent. For screening and ranking purposes, point estimates were generally considered adequate. However, for quantitative use in determining risk profiles for decision making, uncertainty/sensitivity evaluations would be needed.

It was noted that single train unavailabilities will not be flagged as ASP events since they are not required to be reported by 10 CFR 50.73 (LER rule), and suggested that a parallel program to ASP might be desirable to look at these types of failures as a check for PRAs.

Some consideration was also given to potential methods for discovering unknown problems. The limited resources allotted to the ASP program was considered to be a problem in this regard. It was felt that not enough time was devoted to determining the potential implications of events. An approach, similar to "black hatting" in sabotage analysis, was suggested in which individuals would look through the events and try to envision combinations of failures or actions that could lead to problems. The possibility of essentially sampling the PRAs with varied combinations of failures to identify important vulnerabilities was discussed. The approach was felt to provide useful information, but at a high cost. Guided searches for postulated types of failures might be more feasible. A related concept would be to use this approach to search for potential errors of commission.

It was felt that a small advisory committee for ASP would be beneficial. The committee should contain about three experts from different areas (e.g., risk analysis, statistics, and nuclear power plant operations). The group would provide review of methods and issues related to ASP.

It was felt that it is not appropriate to simply wait for events to occur and then evaluate them, but instead, to augment these evaluations with analyses that search for possible problems at plants. A combined approach was felt to be necessary rather than focusing only on operational events evaluation. It was noted that NRC performs the event evaluation portion of this combination, but not the analysis portion. It was felt that plant-specific analysis should be performed in addition to plant-specific event evaluation. It was noted that current NRC priorities in AEOD do not include this activity. The possibility of having the plants themselves perform this analysis was discussed, but the plants suffer from resource limitations. There was also concern that the plants would not give proper credence to events/data from other plants. The need for peer-reviewed PRAs for each plant was aired, but the group in general did not believe this would become a reality.

4. DISCUSSION GROUP 2 - INDUSTRY RISK PROFILE AND GENERIC CONCERNS

Discussion Group 2 treated the issues associated with developing an industry risk profile and also issues with industry trends associated with operational data. The suggested discussion questions are found in Appendix D. Section 4.1 contains a summary of the important information and insights produced by the discussion group, and Section 4.2 contains a more detailed presentation of the information.

4.1 Summary of Discussion Group 2

Discussion Group 2 focused more on generic concerns of event analysis. The group considered methods for assessing the impact and implications that a single event, which occurred at a particular plant, would have on other plants, as well as the evaluation of a group of similar events (trending). The group also considered the feasibility of generating an industry risk profile. In addition, the group discussed the possibility of using IPE/PRA information for improved ASP modeling and in development of an industry risk profile.

PRA or improved ASP methods can be used to assess the importance of the event from a risk perspective. For those events important to risk, the qualitative and quantitative implications of the event must be considered in more detail. The cause(s) of failures should be evaluated.

When evaluating a group of events, analyses must be focused in some manner. One way is to use insights from PRAs and IPEs. Thus, risk-important components, identified from PRAs/IPEs, are candidates for trending studies. For components with large numbers of observations, standard statistical techniques are available to assess trends. Highly reliable components, such as the reactor vessel and batteries, are another group of components which should also be analyzed. Techniques, such as reliability physics methods, can be used to estimate failure rates for these components. The causes of failure should be identified in any analysis, and it is probably better to trend causes rather than failures.

Human performance and common cause failures are other quantities which should be analyzed and trended. Models, such as human reliability models and the cause-defense models, can help in such studies. Again it is important to identify the causes of failure and trend them if possible.

Event analysis can lead to the identification of new phenomena, such as new failure mechanisms which were not recognized in the design process. This type of information is important for any component, especially electronic components, even though the component may not be risk significant. Thus, it is important to monitor the number of failures of components on a regular basis.

The other main topic the group discussed was development of an industry risk profile. The group assumed that severe core damage frequency was the risk measure being trended. The

group felt that IPE results and information may be useful inputs to the development of an industry risk profile. However, caution must be used when combining information from different sources. Some things to consider are: (1) scope of the analyses, (2) quality of the various analyses, (3) assumptions used in the analyses, and (4) analyst-to-analyst variability.

Several concerns were voiced regarding the evaluation of sparse data. When using such data for trending, uncertainty implications must be considered. False trends can appear if uncertainty is not considered in the analysis. It was noted that there is a tendency to consider the occurrence of events as indicating an increased risk, rather than as simply actualizing the predictions. Related to this concern was the tendency to label events as common cause, when again it might simply be realizing the expected number of combined but independent failures. The need for additional guidance and patience when collecting and analyzing operational data was emphasized. It was felt that data are often analyzed in depth before there is sufficient information to produce a meaningful quantitative result. However, qualitative insights can start to develop with small amounts of data.

4.2 Details of Discussion Group 2

The major topics discussed were the use of PRA or ASP-type approaches for screening events (based on their risk importance) to identify those that warrant in-depth evaluation, considerations when trending operational data, and the potential for generating an industry risk profile. Related topics arose and were considered during the process.

For evaluating the potential impact of an event at a plant (screening), the importance results from PRAs were felt to be useful, as long as the affected systems were present in the PRA used for the analysis (e.g., not previously truncated out). The group suggested either an upgraded version of the current ASP methodology or train-level PRAs for evaluating the potential impact of an event at one plant on other plants. Train-level PRAs would be needed rather than the more typical component-level PRAs because operational data is normally reported at the train level. It was felt that the ASP methodology would need to be upgraded to the level that is demanded of PRAs. Particularly, ASP would need to be upgraded to include uncertainty and to improve the treatments of common cause failures and human performance.

The possibility of actually using IPE submittals as the basis for improved models in the ASP program and for generating industry risk profiles was discussed. The information required for the IPE submittal by the utilities would not be sufficient to construct models. The utilities are required to furnish information such as the event trees, dependency diagrams, and dominant sequence results and descriptions; they are not required to furnish fault tree drawings, system unavailabilities, cut set listings (dominant and truncated), etc. Additional difficulties would arise when trying to use IPEs that were developed using different approaches, particularly, small event tree/large fault tree versus large event tree/small fault tree methods. It was noted that data bases are currently being developed for IPE/PRA results which are intended be used to explore the similarities and differences among plants.

Through this work, it might be possible to bin plants, rather than having a separate model for each plant.

In discussing the use of ASP for event evaluation, several points were noted. Attempts were made to compare ASP and PRAs. It was generally agreed that ASP actually represents a conditional PRA, and as such, the same rigor should be demanded of it as PRAs. This would include uncertainty analyses for uses that require quantification, but uncertainty analysis would not be needed for screening purposes. Improved treatment of common cause failures and human performance was also felt to be necessary for ASP. It was noted that good human performance models are not currently available but that there are better treatments than those currently used in ASP. However, no improved treatments were suggested.

Currently, ASP calculates event importance through a conditional core damage probability. This was considered appropriate because of the data scarcity; changes in component failure rates would occur too slowly to be useful. A complementary approach was suggested that would give a different perspective. For a particular event, the impacted equipment would be identified, and then the failure rate would be updated to reflect the occurrence of the failure. Core damage frequencies would then be calculated using the base failure rate and the updated failure rate and compared. This would indicate the risk impact of the event as a change in core damage frequency.

It was suggested that utilities could determine the impact of a particular event on their plant by using the plant's IPE to evaluate the event. It was also suggested that plants could use their IPE to assess the impact of events which occurred at other plants on their own plant. This would be a plant-specific screening of operational events.

The implications of the term "event" were discussed. It was noted that an event can be a complicated set of interrelated failures, a single failure of a component, or the identification of the possibility of a failure of a component without it actually occurring. It was acknowledged that quantifying this last type of event would be very difficult because the applicability of the observed situation to other situations would require the evaluator to make engineering judgments which require information not readily available. In some cases, it was felt that models could be used to aid in this quantification.

A continual loop between ASP-type approaches and snapshot PRAs was suggested in which the PRAs help guide selection and identification of important events. The event analysis leads to updating PRA models and quantification. A difficulty in implementing this process arises because data are reported at the train level, while PRAs are normally modeled at the

component level. However, it was felt that approaches could be developed to include train-level data in a component-level PRA.[8]

When evaluating trends in groups of similar events, techniques such as CUSUM and control charts were suggested for components modeled in PRAs that have relatively large numbers of demands and failures. For highly reliable components, such as the reactor vessel, the scarcity of data would prevent the use of such techniques. For these cases, reliability physics type approaches could be used in which the problem would be decomposed to a level at which a model could be constructed that would be amenable to such methods. Even more difficult would be the evaluation of human performance. The group did not believe current methods adequately model human performance, and that it would probably be quite some time until adequate methods could be developed. However, human performance issues should be flagged for now to compile information on the characteristics of these events so they can be used for improved models on human performance.

The treatment of common-cause failures in trending analyses and for the identification of potentially important generic issues was discussed. It was felt parametric models, such as the β factor model, would not be useful for such studies because they are essentially empirical. A model for the failure would need to be developed using an approach such as the cause-defense framework [2]. Each observed event would be unique, requiring a separate model to describe it. Once a model has been constructed for a particular event, it could be applied across the industry to test for additional occurrences of the problem. Practical considerations limit this approach. That is, it is not feasible to check every plant for each kind of common-cause failure that is identified.

Several concerns were voiced regarding the evaluation of sparse data. First, it was pointed out that it is difficult to trend such data on a plant-specific basis. Statistical methods usually require a moderate number of observations to provide useful results with high confidence. Next, when using data for trending, the uncertainty implications need to be considered. False trends could appear if uncertainty were not considered. On the other hand, some trends can be masked by data uncertainty. It was also noted that there is a tendency to consider the occurrence of events as indicating an increased risk, rather than as simply actualizing the predictions. Related to this concern was the tendency to label events as common cause failures, when again it might simply be realizing the expected number of combined, but independent, failures. Caution must be used when analyzing and interpreting such data. The trends should be updated as new data occur which will increase the understanding and improve the power of the statistical techniques used. It was felt that such data are too often analyzed and conclusions made before there is sufficient information to produce meaningful and credible results.

---

[8] LANL has begun development of approaches that use failure information from components, trains, and systems in the same analysis.

Determining the time interval to use for trending risk was felt to be difficult. If it is too short, the trends might be overly sensitive to very rare events. Longer intervals would damp out such fluctuations, but would not provide insights as rapidly. It was noted that it is easy statistically to say that a trend is present in a set of data, but much more difficult to determine whether or not a risk-significant trend is present when the uncertainties and model limitations are considered. It was stressed that caution is needed when evaluating rare events because prematurely evaluating isolated events can give a false picture.

The sparsity of data was felt to preclude using the ASP results directly to generate an industry risk profile. The previous risk estimates that have been keyed to ASP results were thought to be invalid because of this problem.

It was felt that a reasonable estimate of the industry risk profile might be made by combining the individual plant risks, if the plant submittals for IPE are equivalent to the NUREG-1150 detail. However, it was noted that the basis for such combination would depend on whether or not statistical evaluation of the data and modeling assumptions used in the studies indicated commonality. The group of IPEs/PRAs would ideally be explored to attempt to explain trends and differences before attempting to fit models. Several limitations were noted for this approach of using IPEs/PRAs to estimate an industry risk profile. First, the scope of the IPE analyses would need to be considered when performing evaluations related to the risk profile. In addition, the only the IPE analysis process is being reviewed. The models, data, and results are not being reviewed, introducing question as to their accuracy. The level of detail may vary from plant to plant, making integration of results difficult. The influence of different analysts on the results was felt to be an even more important concern. This problem has been demonstrated in standard benchmark exercises (e.g., Ispra reliability benchmark exercises). Risk profiles would also require updating at selected time intervals to reflect plant changes, operations, and practices.

To be most useful, computerized data bases would need to contain much information not required to be reported in the IPEs. For example, a dependency matrix is needed for each plant at the train level, but it need only be reported at the system level in the IPEs. Among other items, the success criteria used in the IPEs would be needed if it was desired to update results with operational event data. Specific lists of needs were not generated because it was felt that the IPEs will not include the necessary information, and that requests for further information would need to be sent to the utilities. It was also felt that it would be useful if results of importance evaluations were submitted as part of the IPEs.

5. DISCUSSION GROUP 3 - RISK MONITORING AND RISK-BASED PERFORMANCE INDICATORS

The participants in Discussion Group 3 treated the topics of monitoring for trends at an individual nuclear power plant and the feasibility of developing risk-based indicators of plant performance. The suggested discussion questions for this discussion group are found in Appendix E. Section 5.1 contains a summary of the important information and insights produced by the discussion group, and Section 5.2 contains a more detailed presentation of the information.

5.1 Summary of Discussion Group 3

Discussion Group 3 addressed methods for monitoring risk and the development of performance indicators. The strengths and weaknesses of the various characteristics of performance indicators were discussed.

The group felt that risk-based indicators can measure levels of performance vs. goals. However, risk-based indicators usually need to be accumulated over a long period of time (over a year or more) in order to differentiate trends from random variations. In contrast, information for indirect indicators (such as daily power loss) can be collected more frequently, and they can indicate short-term trends. However, the relationship of indirect indicators to safety is not clear. The group felt that both types of indicators are useful to include in a set of performance indicators.

The group concluded that risk-based indicators could be developed for risk-important components. The information needed for those components is out-of-service dates and times and the reasons the components are out of service. Common cause failure (CCF) considerations should also be treated in risk-based indicators since common cause failures are important contributors to risk and system unavailability.

To aid in the use of risk-based indicators, alert levels could be set. The methods to do this included statistics (cumulative, or point-by-point methods), computer simulation (to trade off detection rate versus false alarm rate), and experience (trial and error).

Statistical issues of operational data were also discussed. It was felt that older plant data should always be retained, but it should be treated differently from more recent data. Several possible statistical methods for doing this exist, and should be examined for the best method for the given need.

In establishing a trending interval, the following considerations were identified: the time period needed to detect the trend vs. the rate at which the trend develops, the false alarm rate vs. the detection rate, and the rate of degradation. The need for considering uncertainty properly when determining patterns was noted such that true patterns can be distinguished from those that simply arise from uncertainty.

CCF data needs for risk-based performance indicators were also discussed. LERs would be useful for CCF determination but not necessarily for CCF indication. They are useful for root cause analysis and provide sequence-oriented information. NPRDS gives an understanding of proximate cause of failure. Special search strategies need to be developed for both SCSS and NPRDS to identify potential common cause failures.

5.2 Details of Discussion Group 3

Discussion Group 3 addressed methods for monitoring risk and the development of performance indicators. Before discussing the types of performance indicators that might be used, the group first identified the potential uses of the performance indicators. Most likely, they would be used to judge past performance (assessment indicators) or to project future performance (leading indicators). Assessment indicators could be used both for determining which plants have performed poorly/well and for evaluating whether or not regulations have led to safer plants. It was noted that it is difficult to tell which plants are good/poor performers through assessment indicators, making it even more difficult to validate leading indicators. The group felt that the assessment indicators could be tracked with a higher level of confidence than leading indicators, but acknowledged the need for both.

Both direct and indirect indicators were suggested for these purposes. Direct indicators would have measurable performance that is translated to a risk measure by some risk model. Indirect indicators would not have this direct connection through an analytical model. It was recognized that there would be a spectrum of possibilities between these extremes. The direct indicators can clearly discriminate good and bad performance because of the direct tie to risk, but require a longer time period for data accumulation before trends can be established. Indirect indicators can respond over a shorter time period but suffer from lower credibility.

Several levels of indicators were identified, ranging from the business environment down to train and component level indicators. It would be more difficult to establish credibility when connecting higher level indicators to risk than if using lower level indicators. However, plant-specific indicators at the individual component level would not be practical because the current data collection is inconsistent. With higher level indicators, such as average daily power level, trends could be established during a shorter time window than required for a lower level indicator such as train- or component-level indicators. The group felt that the train level would provide the best compromise, and even that would require additional data reporting.

It was noted that the tradeoffs between the noise, variability, and signal strength of the selected indicator need to be recognized. Methods of grouping data that would increase the signal strength would also increase the noise. The uncertainty in the data sets would need to be considered, both in terms of the tolerance perspective and the confidence perspective in the statistics.

Approaches for using plant-specific PRAs and IPEs in risk monitoring were explored. One possibility would be to use the IPEs and PRAs to determine the importance of safety systems, using the more important systems in the indicator. Then the deviations of the safety system unavailabilities from the values used in the PRAs and IPEs could be tracked. The need for monitoring CCFs and human performance indicators was recognized, but methods for doing this would need to be developed.

To develop indicators on initiating events, the group felt additional research would be needed. However, possible avenues to pursue were discussed. For relatively frequent initiators, the data collected over the past 10 years could be examined for all plants, and attempts made to find patterns for categorizing the events. For rare events, such as ATWS, an approach was suggested that would attempt to identify precursors of the particular event, since data on the event itself would be too scarce. Inspection results might provide information on LOCA precursors.

The frequency for updating the risk assessments used in risk monitoring would depend on a combination of factors. Updates would be necessary after any major plant modification (equipment or procedures) or after a deficiency is found through ASP or other methods. For newer plants, updating would be needed at every refueling because new plants tend to show changes in performance for the first few cycles. Older plants show less variation so would need less frequent updating, but it was suggested that they be updated at least every 5 years.

In updating risk assessment after plant procedural changes, it was felt that the procedures should be considered similar to procedures at a new plant because they are new to the operators. In addition, the possibility of operators tending to fall back on the "old ways" should be considered.

It was suggested that the current set of performance indicators could be made more risk relevant by using a risk weighting of the current indicators. A plant-specific ASP type review of all events could be used.

The group did not currently know how to handle design and manufacturing errors which are not discovered until a design basis reconstitution or improved surveillance test is conducted by the licensee after years of plant operation, but suggested that future research programs examine methods for determining how the discovery of design problems reflects on the number of residual failures in the design. Approaches such as software reliability models that attempt to determine residual defects could be pursued. The importance of keeping reporting non-punitive was stressed, such that the utilities would not be reluctant to report information. It was suggested that the failures be broken into two groups-design and operational.

LERs and NPRDS were viewed as useful for risk-based performance indicators, but not a complete source. LERs would be useful for CCF determination but not necessarily for CCF

indication. They were felt to be useful for root cause analysis, especially if a 30-day report has been made. LERs also provide sequence oriented information. NPRDS does not help identify root causes but does give an understanding of proximate cause and whether the failure dates are clustered together. The engineering data in NPRDS can be somewhat useful for common cause failure analysis because it can be used to locate similar components after a component problem has been identified by other means. Frequency clustering analysis was suggested using NPRDS data, with analysis to identify which portions are from random and non-random phenomena. The non-random portions could be examined for common-cause failure. The failure records in NPRDS could be used to identify potential common-cause component groups, and the work maintenance records could be used to determine the actual cause of the failure.

Statistical issues of operational data were also discussed. The group believed that older plant data should always be retained, but treated differently from more recent data. Several possible methods for doing this exist. The key concern was choosing a method that discounts but does not discard old data. It was felt that there is no general way for establishing intervals for developing trends, but in developing a specific interval one should consider the time period needed to detect the trend vs. the rate at which the trend develops, the false alarm rate vs. the detection rate, and the rate of degradation.

Several means for establishing alert levels were identified: percentile, CUSUM, computer simulation, or a brute force approach which starts broad and narrows in. The level depends on the false alarm rate, the significance of the false positives and false negatives, and the risk of the item.

The importance of considering uncertainty properly when determining patterns was noted. Without it, true patterns can not be distinguished from those that simply arise from uncertainty. It was felt that more rigorous statistical review of current methods was needed for establishing trend intervals.

The group also discussed whether or not suspected outliers should be considered in evaluations, and suggested an approach. First, the group characteristics must be determined using all data for the plants in a group. Then statistical analysis could be used to determine if the suspected outliers are truly outliers or if they are points on the tails of the distributions. If the suspected outlier is shown not to be an outlier, it should be considered a generic issue, with regulation focused on reducing the variability of the group. On the other hand, if it is shown to be an outlier, it should only be considered for the plant-specific evaluation.

6. OVERALL INSIGHTS

The comments expressed in this section were not compiled at the Workshop; they were prepared after careful reading of the notes taken during the discussion groups and listening to the recordings of the actual discussion sessions.

(1) General

- It was recognized that it is not feasible to treat all events, but that certain classes of events should be flagged for further review.

- Statistical methods have been demonstrated for trending and as performance indicators for relatively frequent events, but reactor safety concerns often involve sparse data. Data scarcity prevents direct use in many cases, but decomposition to a lower level might make analyses possible. It was repeatedly emphasized that care must be exercised when analyzing scarce data or false conclusions may be drawn.

- A common problem identified during the workshop was that NRC needs and uses of analyses were often not well understood. That is, the roles of ASP, trending analyses, performance indicators, etc., in NRC functions were not generally understood by the workshop participants.

- There was a general impression that current evaluations of operational data will not likely identify "what we don't know." Increased NRC priority would be needed to focus resources on this broader question to identify appropriate methods to perform such analyses in a systematic way.

- A universal message from all of the discussion groups was to use risk insights from PRAs and IPEs to focus trending studies, etc.

- Events which are important from PRA insights should be flagged. Such conditions are events which become important when coupled with an external initiator (e.g., fire, flood, earthquake), containment performance considerations, etc.

- Common cause failures and human performance concerns were identified as important issues to be further studied in trending analyses and in upgrading of the ASP models.

(2) Accident Sequence Precursors

- There was a general feeling that the ASP program is useful, but that it needs improvement in system modeling, treatment of common cause failures, and

treatment of human performance. Plant-specific, train-level models would meet this need.

- In the ASP program conditional core damage probabilities are calculated for certain events. However, the occurrence rate of the precursor event itself is generally not calculated. The frequency of precursor events could also be useful as a check on expected occurrence rates based on PRA estimates.

(3) Generic/Risk Profile

- IPE analyses would be a useful source of information for fulfilling many needs (e.g., developing plant-specific, train-level models, developing an industry risk profile). However, it was realized that much of the information needed for ASP and other uses is not required to be submitted to the NRC in the IPE submittal.

- It was felt that it would be possible for the NRC to develop an industry risk profile. If it is done, it will require careful scoping and planning before developing the methods and its implementation.

(4) Performance Indicators

- Risk-based performance indicators should be developed using risk-important component and systems. This effort would require new models and data.

(5) Other

- Data reporting was overwhelmingly felt to be a weakness. Information that would make the failure records more useful include: mode of operation at time of failure, more complete failure narratives, better root cause information, time of failure, time equipment was restored to service.

7. REFERENCES

1. J. W. Minarick, et al, **Precursors to Potential Severe Core Damage Accidents: 1990; A Status Report**, NUREG/CR-4674, Volumes 13 and 14, August 1991.

2. H.M. Paula, et al, **A Cause-Defense Approach to the Understanding and Analysis of Common Cause Failures**, NUREG/CR-5460, March 1990.

3. S. Kaplan, "On a 'Two-Stage' Bayesian Procedure for determining Failure Rates from Experimental Data," **IEEE Trans. on Power Apparatus and Systems,** PAS-102, 195-202, 1983.

4. G. Apostolakis, "The Concept of Probability in Safety Assessments of Technological Systems," **Science,** 250, 1359-1364, 1990.

5. G. Apostolakis, S. Kaplan, B.J. Garrick, and W. Dickter, "Assessment of the Frequency of Failure to Scram in LWRs," **Nuclear Safety,** 20, 690-705, 1979.

6. N. Siu and G. Apostolakis, "A Methodology for Analyzing the Detection and Suppression of Fires in Nuclear Power Plants," **Nuclear Science and Engineering,** 94, 213-226, 1986.

7. D.L. Sanzo and G. Apostolakis, "A Time-Dependent Methodology for Evaluating Component Reliability," **Proceedings of the International Nuclear Power Plant Aging Symposium,** Bethesda, MD, August 30 - Sept. 1, 1988, NUREG/CP-0100.

8. J. Reason, **Human Error,** Cambridge University Press, New York, 1990.

APPENDIX A

List of Workshop Attendees

LIST OF WORKSHOP ATTENDEES

George Apostolakis, UCLA
University of California
38-137 Engineering IV
Los Angeles, CA 90024-1597
(310) 825-1300

Cory Atwood, INEL
EG&G Idaho, Inc.
MS: 3421
PO Box 1625
Idaho Falls, ID 83415
(208) 526-0431

Mohammad Ali Azarm, BNL
Building 130
Upton, Long Isand NY 11973
(516) 282-4992

Pat Baranowsky, AEOD
MNBB-9112
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 492-4480

Bill Beckner, NRR
OWFN-10E4
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 504-1089

Vic Benaroya, AEOD
MNBB-9112
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 492-8318

Dennis Bley, PLG
4590 MacArthur Blvd.
Suite 400
Newport Beach, CA 92660
(714) 833-2020

Bennett Brady, AEOD
MNBB-9112
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 492-4499

James Bryce, INEL
EG&G Idaho, Inc.
MS: 2407
PO Box 1625
Idaho Falls, ID 83415
(208) 526-8231

Robert Budnitz, FRA
2000 Center Street
Suite 418
Oakland, CA 94704
(510) 644-2700

Allen Camp, SNL
Division 6412
PO Box 5800
Albuquerque, NM 87185
(505) 844-5960

Al Chaffee, NRR
OWFN-11A1
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 504-1168

Mike Cullingford, NRR
OWFN-12G18
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 504-1276

Mark Cunningham, RES
NLS-372
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 492-3965

John Darby, SEA
6100 Uptown Blvd., NE
Albuquerque, NM 87110
(505) 884-2300

Bob Dennig, NRR
OWFN-11A1
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 504-1156

Susan Dingman, SNL
Division 6412
PO Box 5800
Albuquerque, NM 87185
(505) 844-0099

Joe Fragola, SAIC
8 West 40th Street
14th Floor
New York, NY 10018
(212) 764-2820

Bill Galyean, INEL
EG&G Idaho, Inc.
MS: 2405
PO Box 1625
Idaho Falls, ID 83415
(208) 526-0627

Cindy Gentillon, INEL
EG&G Idaho, Inc.
MS: 3421
PO Box 1625
Idaho Falls, ID 83415
(208) 526-9891

Jack Heltemes, RES
NLS-007
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 492-3720

Don Hickman, AEOD
MNBB-9112
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 492-4431

Tom Ippolito, SEA
1700 Rockville Pike
Suite 400
Rockville, MD 20852
(301) 468-7371

Carl Johnson, RES
NLS-316
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 492-3548

Bill Jones, AEOD
MNBB-9715
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 492-4442

Ed Jordan, AEOD
MNBB-3701
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 492-4848

Ernie Lofgren, SAIC
1710 Goodridge Drive
Tier 2-7-1
McLean, VA 22102
(703) 821-4492

Erasmia Lois, RES
NLS-372
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 492-3557

Steve Long, NRR
OWFN-10E4
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 504-1077

Fred Manning, AEOD
MNBB-9715
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 492-4426

Harry Martz, LANL
Statistics Group (A-1)
Analysis and Assessment Division
Los Alamos, NM 87545
(505) 667-2687

Gary Mays, ORNL
Bldg. 9201-3
PO Box 2009
Oak Ridge, TN 37831-8065
(615) 574-0394

Steve Mays, ACRS
P-315
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 492-7904

Joe Minarick, SAIC
708 So. Illinois Ave.
Suite E-103
Oak Ridge, TN 37830
(615) 482-6743

Tom Mitchell, INPO
Suite 1500
1100 Circle 75 Parkway
Atlanta, GA 30339-3064
(404) 953-5439

Mohammed Modarres
Building 090
Nuclear Engineering
College Park, MD 20742-2115
(301) 405-5226

Ali Mosleh, U of MD
Building 090
Nuclear Engineering
College Park, MD 20742-2115
(301) 405-5215

Tom Novak, AEOD
MNBB-9112
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 492-4484

Pat O'Reilly, AEOD
MNBB-9112
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 492-8858

Gareth Parry, NUS
910 Clopper Road
Gaithersburg, MD 20878
(301) 258-2536

Henrique Paula, JBFA
1000 Technology Park Center
Knoxville, TN 37932
(615) 966-5232

Arthur Payne, SNL
Division 6412
PO Box 5800
Albuquerque, NM 87185
(505) 844-7321

Marie Pohida, NRR
OWFN-10E4
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 504-1846

Mike Poore, ORNL
Bldg. 9201-3
PO Box 2009
Oak Ridge, TN 37831-8065
(615) 574-0325

Dale Rasmuson, AEOD
MNBB-9112
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 492-4490

Stacey Rosenberg, NRR
OWFN-10E4
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 504-1082

Jack Rosenthal, AEOD
MNBB-9715
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 492-4440

Denny Ross, AEOD
MNBB-3701
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 492-7361

Pranab Samanta, BNL
Building 130
Upton, Long Isand NY 11973
(516) 282-4948

Howard Stromberg, INEL
EG&G Idaho, Inc.
MS: 2407
PO Box 1625
Idaho Falls, ID 83415
(208) 526-9167

Lillian VanSaten, NRC
W-308
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 492-8938

Gary Wilson, INEL
EG&G Idaho, Inc.
MS:
PO Box 1625
Idaho Falls, ID 83415
(208) 526-9511

Millard Wohl, NRR
OWFN-11E22
Nuclear Regulatory Comm.
Washington, DC 20555
(301) 504-1181

John Wreathall
4157 MacDuff Way
Dublin, OH 43017
(614) 791-9264

Robert Youngblood, BNL
Building 130
Upton, Long Isand NY 11973
(516) 282-2363

APPENDIX B

NRC Programs for Evaluating Operating Data

Operational Experience and Evaluation

Actual operating experience is an essential input to the regulatory process for assuring that licensed activities are conducted safely. Major data sources are reports submitted by licensees to the NRC in compliance with 10 CFR 50.72 ("Immediate Notification Requirements for Operating Nuclear Power Reactors"), 10 CFR 50.73 ("Licensee Event Report System"), and voluntary reports of component failures submitted to the Nuclear Plant Reliability Data System (NPRDS), which is managed by the Institute of Nuclear Power Operations (INPO). These data are maintained in computerized data bases.

Additional sources of data include (1) licensees' monthly operating reports, (2) NRC inspection reports (regional reports as well as reports from special evaluations performed by Augmented Inspection, Incident Investigation, and Diagnostic Evaluation Teams), (3) 10 CFR Part 21 reports ("Reporting of Defects and Noncompliance"), (4) preliminary notifications of events issued by the NRC, and (5) foreign reactor events received through international exchange of information. The NRC also obtains operational data from site visits, and from licensee responses to bulletins, generic letters, and 10 CFR 50.54(f) letters. Data for NRC sponsored probabilistic risk analyses (PRAs) are usually obtained from site visits, but "generic" sources may also be used.

Specified safety criteria are used to identify events which are Abnormal Occurrences to be reported to Congress (Table 1), significant events for the NRC Performance Indicator Program (Table 2), important events for engineering analyses and assessments by AEOD's Reactor Operations Analysis Branch (Table 3), and precursors to potential severe core damage accidents (Table 4) as identified by the Accident Sequence Precursor (ASP) program.

Information on file in the NPRDS is derived from engineering and failure data submitted by nuclear power plant licensees to INPO. The NPRDS produces failure statistics on components and systems related to nuclear safety. Such statistics are for use in deriving implied "reliability" of components which may be of interest to operators and designers of nuclear power plants, reactor manufacturers, architect-engineering and constructor firms and regulatory agencies. However, the data is not sufficient to perform actual reliability and availability analyses because of limitations in raw data required to be reported to the system. The NRC considers the NPRDS to be a vital adjunct to the LER system. Its value as an analytic tool is directly dependent upon the accuracy and completeness of the data, and the degree of industry participation. For 64 plants reviewed by INPO in 1989 and 1990 and one in 1991, the mean completeness of component failure reporting was 70 percent and the median 81 percent.

The primary source of data on operational events used in both routine evaluations and special studies are licensee event reports (LERs). For 1991, about 2000 LERs will be submitted covering events with a wide range of significance (e.g., spurious HVAC isolations to reactor scrams with complications). About 150 related pieces of data for each LER are

entered into the Sequence Coding and Search System (SCSS) data base. The SCSS facilitates the storage and retrieval of information about each event (e.g., causal and time aspects of occurrences within the event sequence). This system is maintained by Oak Ridge National Laboratory. A separate data base is maintained at the Idaho National Engineering Laboratory (INEL); this data base is used to support studies for specific kinds of events and the NRC Performance Indicator Program. The data base is derived from LERs, 10 CFR 50.72 reports, and licensees' monthly operating reports and contains operational information such as ESF actuations (including reactor scrams), safety system failures, technical specification violations and shutdowns, and reactor critical hours.

Operational data are reviewed and evaluated to identify (1) significant events and any associated safety concerns and root causes, (2) the trends and patterns displayed by these events, (3) the adequacy of the corrective actions taken to address these concerns, and (4) the generic applicability of events and concerns to other plants.

The ASP method models and evaluates plant equipment and human responses that could affect the progression of an accident, evaluating the actual failures that have occurred along with the probabilities for postulated additional failures that could occur. The precursor method uses event tree models to evaluate the likelihood of various possible outcomes (scenarios) for the events being modeled, resulting in a quantitative estimate of the significance of the event in terms of conditional probability of core damage. The overall ASP analysis process is shown in Figure 1. The precursor event evaluations are presented in ASP NUREG reports which are published annually. The breakdown of precursor events by event type and significance are plotted and provided to the Commission each year to show trends. Summary information on precursor events are given to NRC senior management to provide another perspective on plant operating experience. NRR has adopted the ASP methodology for evaluation of selected 10 CFR 50.72 reports to assist in the identification of significant events. The ASP models in use by NRR were reviewed and modified to bring them into better quantitative agreement with available PRAs, and ATWS event trees were added.

Certain shortcomings of the existing ASP models are being addressed by NRR and their subcontractors SAIC and ORNL. For example, when evaluating certain events, modeling deficiencies can cause overly conservative estimates of conditional core damage probability. One deficiency concerns not giving proper credit for alternate long-term means of core decay heat removal and a second deficiency concerns not properly crediting the charging pumps as an alternate to the HPI pumps on certain plants. Additional event trees are also being developed for steam generator tube rupture and ATWS. In addition to correcting known problems, an effort is underway to confirm that ASP modeling of plant system configurations and capabilities are correct and current by verifying them using information from individual plant examination submittals.

Trends and patterns analyses are performed to (1) identify and provide a quantitative context for new safety issues; (2) evaluate the effectiveness of current regulations, regulatory

actions and initiatives taken by licensees to resolve safety issue concerns; and, (3) help guide and focus engineering evaluations. PRA insights can be helpful to identify components, systems, accident initiators, accident sequences and safety/regulatory issues as candidates for trends and patterns analyses. Also, PRA assessments can be helpful to evaluate the safety significance of the results of trends and patterns analyses.

NRR has begun trending the results of the ASP evaluations published annually by AEOD. A summary is made of the conditional probabilities for the precursor events for each year. The total numbers of precursor events per year and the numbers of events exceeding various values have also been considered. The ASP report data was also scrutinized for apparent differences associated with plant age, size of utility company, types of reactors, etc.

The NRC Performance Indicator (PI) Program is another aspect of efforts to monitor the performance of nuclear power plant licensees. This program currently monitors individual plant as well as industry-wide data on eight PIs and evaluates the data to determine performance trends. The eight PIs are (1) the number of unplanned automatic reactor scrams (trips) while a reactor is critical, (2) the number of safety system actuations, (3) the number of significant events, (4) the number of safety system failures, (5) the forced outage rate, (6) the number of equipment-forced outages per 1000 commercial critical hours, (7) the collective radiation exposure, and (8) cause codes. Most of these PIs are generated by the NRC's computerized data bases. The trends of the PIs are shown on a plant-specific basis, as well as comparisons to industry-wide averages. These reports are issued quarterly. In the fourth quarter report each year, annual industry trends for each PI for the past several years are presented. Figure 2 shows the trends in the industry averages for the first seven PIs for the years of 1986 through 1990. (Industry-wide averages are not calculated for the cause code PI.)

The PIs are intended to monitor plant operational safety performance. Therefore, they should reflect trends in one of the following three key elements of operational safety: (1) frequency of transients, (2) unavailability of safety systems, and (3) potential for common-cause failures. The development of a risk-based indicator of key safety systems unavailability has been studied for some time but has not been implemented because the needed data is not currently available to the NRC on a routine basis.

The NRC has developed state-of-the-art software computer systems for use in risk analyses. The Integrated Reliability and Risk Analysis System (IRRAS) is used to perform a level 1 PRA. Event trees and fault trees are developed and analyzed using IRRAS. IRRAS is being used in the preparation of low power/shutdown PRAs. The System Analysis and Risk Assessment (SARA) software is designed to perform sensitivity studies on cut sets. These programs provide new tools for the NRC to use in ASP studies and event evaluations. The NRC is also loading data from PRAs into the MAR-D data base for use with IRRAS and SARA. So far about 8 PRAs have been loaded into the data base. The key to using IRRAS and SARA effectively in NRC applications is to develop the event tree and fault tree models to take advantage of the unique features of the codes.

Table 1
Abnormal Occurrence Criteria

The following criteria for abnormal occurrence determinations were set forth in an NRC policy statement published in the Federal Register on February 24, 1977 (Vol. 42, No. 37, pages 10950-10952).

An event will be considered an abnormal occurrence if it involves a major reduction in the degree of protection of the public health or safety. Such an event would involve a moderate or more severe impact on the public health or safety and could include but need not be limited to:

1. Moderate exposure to, or release of, radioactive material licensed by or otherwise regulated by the Commission;

2. Major degradation of essential safety-related equipment; or

3. Major deficiencies in design, construction, use of, or management controls for licensed facilities or material.

Examples of the types of events that are evaluated in detail using these criteria are:

For All Licensees

1. Exposure of the whole body of any individual to 25 rem or more of radiation; exposure of the skin of the whole body of any individual to 150 rem or more of radiation; or exposure of the feet, ankles, hands or forearms of any individual to 375 rem or more of radiation [10 CFR 20.403(a)(1)], or equivalent exposures from internal sources.

2. An exposure to an individual in an unrestricted area such that the whole body dose received exceeds 0.5 rem in one calendar year [10 CFR 20.105(a)].

3. The release of radioactive material to an unrestricted area in concentrations which, if averaged over a period of 24 hours, exceed 500 times the regulatory limit of Appendix B, Table II, 10 CFR Part 20 [CFR 20.403(b)(2)].

4. Radiation or contamination levels in excess of design values on packages, or loss of confinement of radioactive material such as (a) a radiation dose rate of 1000 mrem per hour three feet from the surface of a package containing the radioactive material, or (b) release of radioactive material from a package in amounts greater than the regulatory limit.

Table 1 (cont.)

5. Any loss of licensed material in such quantities and under such circumstances that substantial hazard may result to persons in unrestricted areas.

6. A substantiated case of actual or attempted theft or diversion of licensed material or sabotage of a facility.

7. Any substantiated loss of special nuclear material or any substantiated inventory discrepancy that is judged to be significant relative to normally expected performance and that is judged to be caused by theft or diversion or by substantial breakdown of the accountability system.

8. Any substantial breakdown of physical security or material control (i.e., access control, containment, or accountability systems) that significantly weakened the protection against theft, diversion, or sabotage.

9. An accidental criticality [10 CFR 70.52(a)].

10. A major deficiency in design, construction, or operation having safety implications requiring immediate remedial action.

11. Serious deficiency in management or procedural controls in major areas.

12. Series of events (where individual events are not of major importance), recurring incidents, and incidents with implications for similar facilities (generic incidents) at create major safety concern.

For Commercial Nuclear Power Plants

1. Exceeding a safety limit of license technical specifications [10 CFR 50.36(c)].

2. Major degradation of fuel integrity, primary coolant pressure boundary, or primary containment boundary.

3. Loss of plant capability to perform essential safety functions such that a potential release of radioactivity in excess of 10 CFR Part 100 guidelines could result from a postulated transient or accident (e.g., loss of emergency core cooling system, loss of control rod system).

4. Discovery of a major condition not specifically considered in the safety analysis report (SAR) or technical specifications that requires immediate remedial action.

Table 1 (cont.)

5. Personnel error or procedural deficiencies that result in loss of plant capability to perform essential safety functions such that a potential release of radioactivity in excess of 10 CFR Part 100 guidelines could result from a postulated transient or accident (e.g., loss of emergency core cooling system, loss of control rod system).

Table 2
Criteria for Significant Events for the Performance Indicator Program

Events normally involving one or more of the following:

1. The degradation of important safety equipment.

2. An unexpected plant response to a transient or a major transient itself.

3. A degradation of fuel integrity, the primary coolant pressure boundary, or important associated structures.

4. A reactor trip with complications.

5. An unplanned release of radioactivity exceeding plant Technical Specifications (TS) or regulations.

6. Operation outside the limits of TS.

7. Other events that are considered significant.

Table 3
AEOD Reactor Operations Analysis Branch Screening Criteria for Important Events

Events are assigned to one of four categories depending on its safety importance in accordance with the following criteria:

Category 1 - Those events of such obvious importance that actions should be initiated immediately by AEOD or other office or organization to ensure plant safety.

Category 2 - Those events (or combination of events) which appear to have safety importance but do not require immediate action to ensure plant safety.

Category 3 - Those events (or combinations of events) which require additional consideration by another ROAB Section to permit assignment to Categories 1, 2, or 4.

Category 4 - Those events with little apparent importance to safety.

The criteria used to help identify such events, for operating occurrences and for operating conditions, are listed below. The final determination of significance is based on engineering judgment.

Operating Occurrence Criteria

A. Safety limit violated

B. Alert or higher emergency classification

C. On-demand failure of safety system

D. Actual unexpected performance

E. Common-mode/cause failure

F. System interaction

G. Human errors

H. Natural phenomenon

I. Scram/transient/ESF actuation with complications

J. Scram/transient/ESF actuation with equipment operable

K. Personnel overexposure or injury

L. Release of radioactivity

M. An accident

N. Moderate frequency event with the potential for severe core damage

O. Other

Table 3 (cont.)

Operating Condition Criteria

A.	Condition which could initiate an accident or prevent successful mitigation	F.	Procedural or training errors
B.	Outside design basis or requirements	G.	Potential failure or degradation of safety equipment
C.	Potential unexpected failure or response	H.	Management deficiencies
D.	Potential common-mode/ cause failure	I.	Technical specification violation
E.	Potential system interaction	J.	Programmatic deficiencies

Table 4
Typical Events Evaluated by ASP Process

- Unexpected core damage initiators (LOOP and small-break LOCA)
- All events in which reactor trip was demanded and a safety-related component failed
- All support system failures, including failures in cooling water systems, instrument air, instrumentation and control, and electric power systems
- Any event where two or more failures occurred
- Any event or operating condition that was not predicted or that proceeded differently from the plant design basis
- Any event that, based on the reviewers' experience, could have resulted in or significantly affected a chain of events leading to potential severe core damage

The overall precursor selection process is shown in Figure 1.

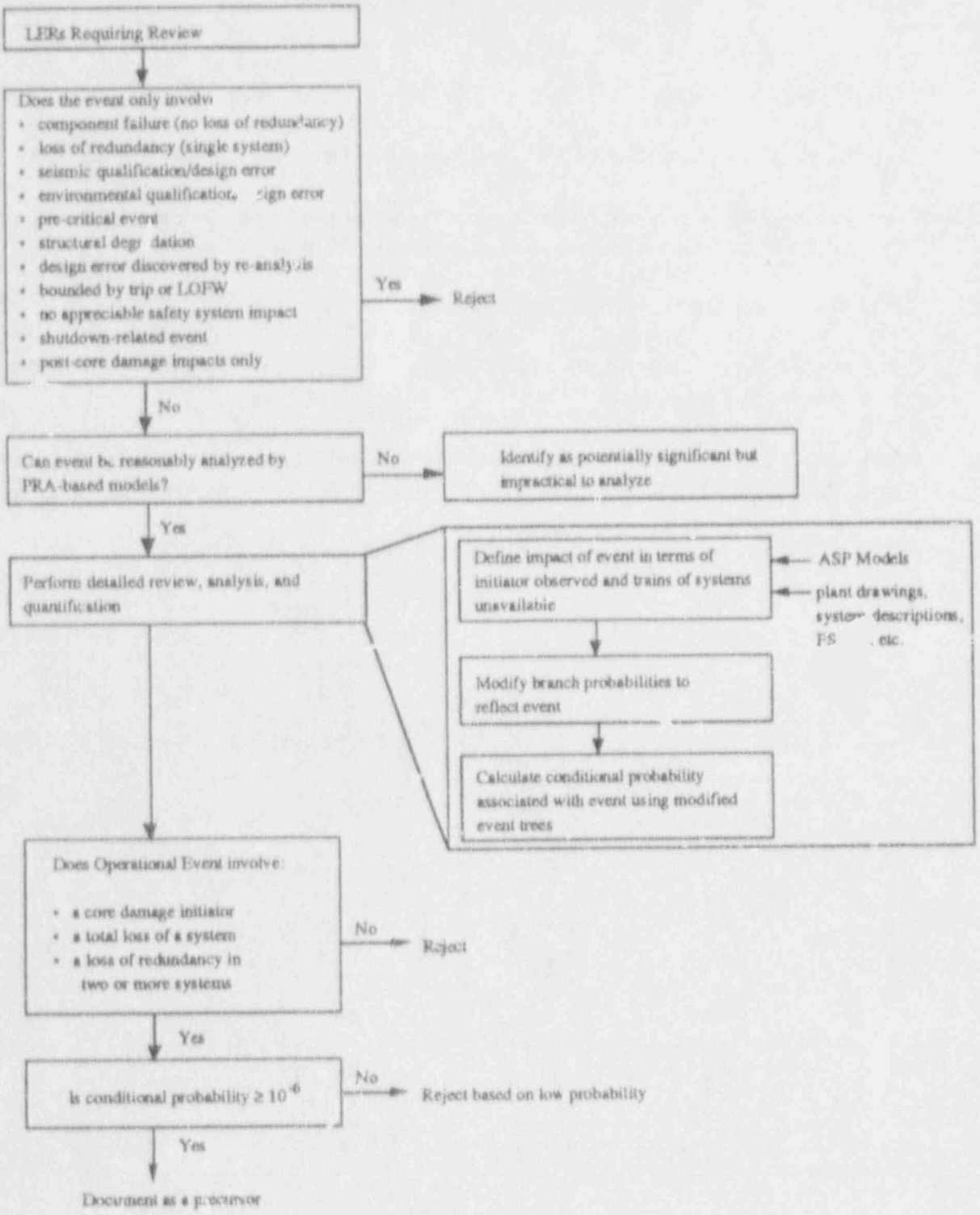


Figure 1. ASP Analysis Program

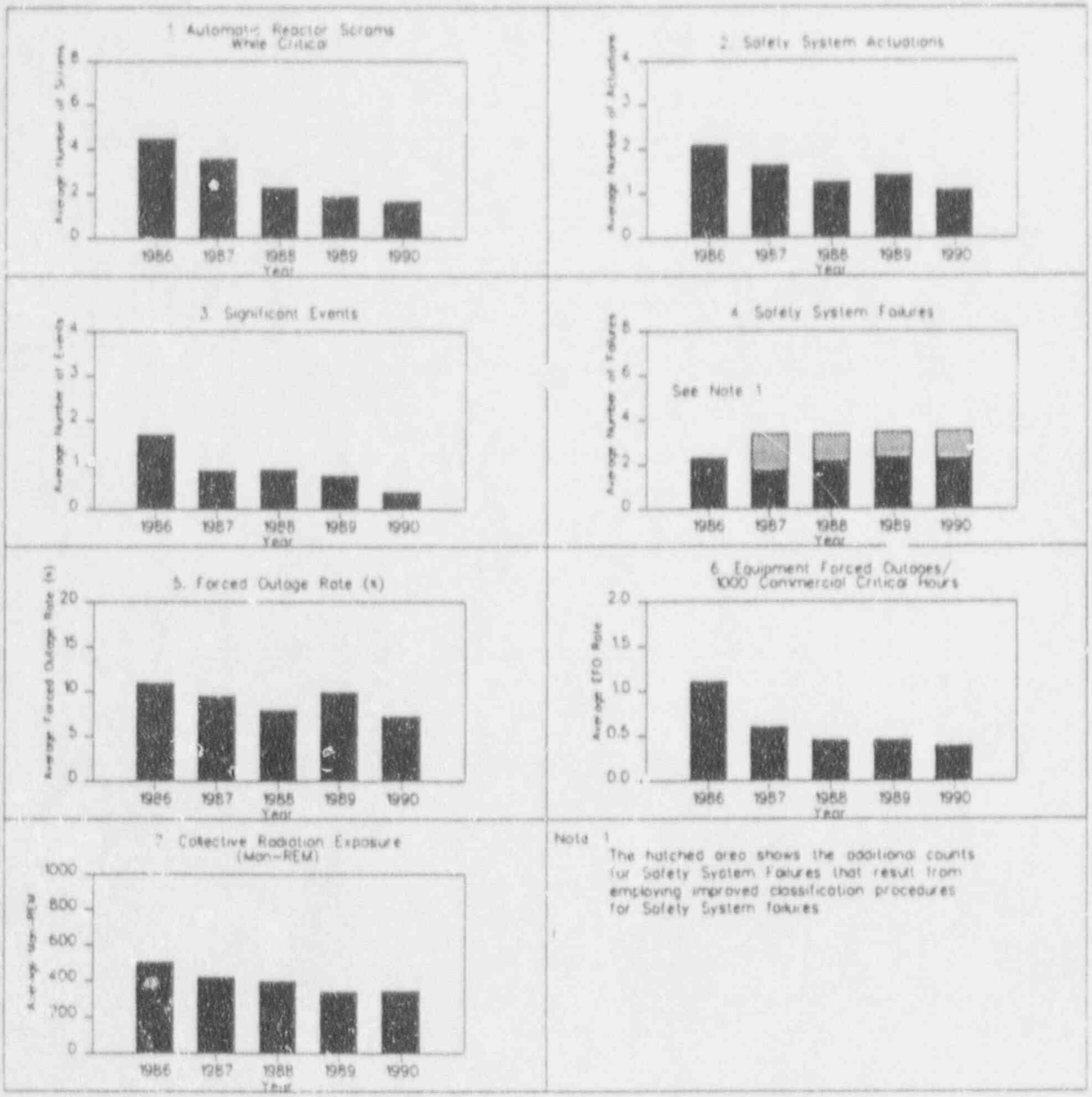


Figure 2. Annual Industry performance averages -- 1986-1990

APPENDIX C

Discussion Group 1 Questions and P· ·ticipants

WORKSHOP DISCUSSION GROUP 1
Risk Significance of Events

1. What fundamental screening and modeling aspects of ASP should be reevaluated and improved to increase confidence that important events are not being missed because of biases introduced by the methodology and its implementation, or by limitations in ASP models?

2. What level of modeling detail should be included in computer codes for ASP analyses?

3. What importance measures should be used and how should they be used to identify event significance?

4. How can ASP be extended to external events: (1) Fire; (2) Internal flood; (3) Seismic; etc?

5. What kind of human performance evaluation improvements should be made to, or incorporated in ASP models/procedures?

6. What can be done to improve ASP analysis efficiency to speed up the process? Can screening criteria and qualitative assessments be developed to reduce the number of detailed ASP/PRA evaluations, especially for those of very low conditional core damage probability.

7. What are the statistical limitation and problems associated with trending ASP results?

8. [illegible] statistical limitations important when ASP results are used to display an [illegible] trend?

9. [illegible] the uncertainties in ASP? How should uncertainty be factored in to intended [illegible] SP results? How should they be handled? Qualitative treatment versus quantification.

10. What kinds of extrapolations can be done with quantitative and qualitative ASP results?

11. How can/should ASP results be factored into PRAs/IPEs?

12. Is it practical to use PRAs/IPEs for event (ASP) analysis? How should PRA models and results be structured in order to be most useful for event analysis? What data is needed?

13. What is the minimum information needed to perform a credible risk assessment of an event? What kind of changes should be made to event reporting (50.72/73) to help assure important events will be identified by the ASP screening process?

DISCUSSION GROUP 1 PARTICIPANTS

Moderator:	Allen Camp, SNL
Participants:	Bill Jones, AEOD
	Fred Manning, AEOD
	Joe Mibarick, SAIC
	John Darby, SEA
	Bob Budnitz, FRA
	Steve Long, NRR
	Marie Pohida, NRR
	Gary Wilson, INEL
	Steve Mays, ACRS
	Cory Atwood, INEL
	Mike Cullingford, NRR

APPENDIX D

Discussion Group 2 Questions and Participants

WORKSHOP DISCUSSION GROUP 2
Industry Risk Profile and Generic Concerns

1. How can we use common cause failure, systems interactions, and human performance analysis methodology to analyze industry wide data for trends, and for the identification of potentially important generic issues? What methodologies are most suitable? What data detail is required?

2. What approaches and methodologies can we use to cull the LER and NPRDS data bases to identify risk significant industry trends: at the component level; at the system level; at the event level; at the issue level? (other?) How can information from all or a group of plants be used to identify potentially risk significant problems? What other data sources should be routinely screened? How can we combine or extrapolate from and between LER and NPRDS (or other) data bases to form the most complete picture?

3. What methodology and criteria should be used to select a class of events (component, system, issue level) for detailed study (e.g. statistical, risk, root cause and engineering evaluations)?

4. Given the nature of the events reported in the available data bases, what statistical techniques should be used for analyzing trends?

5. If it were possible to develop a nuclear industry risk profile, what are some ways it could be done and what should it include?

6. Given some form of risk estimate is or will be available for most plants, how can they be combined to provide an industry risk profile? What technical issues need to be addressed and what approaches and methods should be used or developed for this application?

7. What approach might be developed using available PRAs and IPE results to generate a periodic, industry risk profile update (trend). What data would be needed?

8. What information from PRAs and IPEs should be catalogued in a computerized data base?

9. What are the pros and cons of using ASP results to identify industry historic risk trends. What are the statistical issues associated with this? What are the statistical implications, confidence level in results?

DISCUSSION GROUP 2 PARTICIPANTS

Moderators:	Gareth Parry, NUS
	Ali Mosleh, Univ. of MD
Participants:	Pat O'Reilly, AEOD
	Bennett Brady, AEOD
	George Apostolakis, UCLA
	Henrique Paula, JBFA
	Bob Dennig, NRR
	Howard Stromberg, INEL
	Ali Azarm, BNL
	Harry Martz, LANL
	Dale Rasmuson, AEOD
	Jack Rosenthal, AEOD
	Bill Beckner, NRR
	Mark Cunningham, RES
	Tom Novak, AEOD

APPENDIX E

Discussion Group 3 Questions and Participants

WORKSHOP DISCUSSION GROUP 3
Risk Monitoring and Risk-Based Performance Indicators

1. If we were to start from scratch with no preconditions, what types of performance indicators should be selected to monitor plant safety/risk? What data would be needed? What practical alternatives are there?

2. What approach should be taken to identifying and developing surrogate or indirect indicators for plant risk monitoring?

3. What approaches and methods could be developed and used to employ plant specific PRAs and IPEs as a risk monitoring tool? Should total risk be monitored or should specific components and systems be monitored? What about monitoring certain component types, or human performance indicators? What types of indicators should be developed for initiating events?

4. How often should the risk assessment, or specified elements of it (e.g. system reliability) that are used for risk monitoring be updated? What data would be required?

5. What risk methodology might be used to improve the current set of performance indicators? Can they be made more risk relevant?

6. How should we treat design and manufacturing errors which were not discovered until a design basis reconstitution or improved surveillance test was conducted by a licensee after years of plant operation.

7. How can we utilize existing LER and NPRDS data in combination to improve on their usefulness in meeting risk-based performance indicator data needs? What other data might be used to fill voids that are inherent to these data sources? Optimally, what data is needed?

8. What statistical issues should be addressed when developing and implementing risk-based performance indicators? What methods are best suited for routine periodic trending (e.g. rolling average, regression) of risk-based indicators? What approach should be used to select intervals for developing trends? When is past history to old to be considered indicative of current performance?

9. What methods should be used to establish alert levels when monitoring risk? How can we identify significant trends? What method or approach should be used to differentiate actual short term deviations in performance from random variations?

10. How can we spot patterns of events that point to problems at a particular plant?

DISCUSSION GROUP 3 PARTICIPANTS

Moderator:	Joe Fragola, SAIC
Participants:	Don Hickman, AEOD
	Mike Poore, ORNL
	Dennis Bley, PLG
	Cindy Gentillon, INEL
	Bill Galyean, INEL
	Arthur Payne, SNL
	Carl Johnson, RES
	Erasmia Lois, RES
	Pranab Samanta, BNL
	Ernie Lofgren, SAIC
	Millard Wohl, NRR
	John Wreathall, SAIC
	Stacy Rosenberg, NRR
	Tom Novak, AEOD

APPENDIX F

View Graphs

for

"Accident Sequence Precursor Program Methods"

Joseph W. Minarick

ACCIDENT SEQUENCE PRECURSOR PROGRAM METHODS

Workshop on the Use of PRA Methodology for the
Analysis of Reactor Events and Operational Data

January 29-30, 1992

Joseph W. Minarick
Science Applications International Corporation

1

Definitions

Accident sequences of primary interest in the ASP program are those that, if completed, would have resulted in inadequate core cooling and would have potentially resulted in severe core damage.

Accident sequence precursors are events that are important elements in such sequences -- for example, an unusual initiating event or failures of multiple components that, when coupled with one or more postulated events, could result in a plant condition leading to severe core damage.

2

Objectives

Search operational events for the elements or precursors of severe core damage accident sequences.

Analyze operational events and rank them as to their likelihood of proceeding to core damage.

From operational events identify significant or important sequences that, more likely than others, could lead to severe core damage.

Type of Events Covered

While all off-normal plant conditions are associated with some risk, the ASP program concentrates on:

- Unusual initiating events (loss of offsite power, small break loss of coolant accident, cascade electrical failures),
- Total failures of safety-related systems, and
- Degraded multiple systems

Types of Events Not Covered

Events not addressed include:

- Uncomplicated reactor trips,
- Losses of feedwater without additional failures,
- Single failures in systems (without an initiating event),
- Losses of redundancy in a single system which could be a system failure at another plant (e.g., unavailability of a motor-driven and turbine-driven AFW pump at a plant with a three-pump AFW system), and
- Design errors discovered by reanalysis.

Overall ASP Program Approach

Review LERs to identify events which satisfy selection criteria as precursors.

Determine impact of "elements" of each event on systems and functions which provide protection against core damage. These systems and functions are defined through the use of event sequence models (event trees).

Estimate a conditional probability of subsequent severe core damage for each precursor using event trees modified to reflect systems observed to be degraded or failed during the precursor. Initiating event frequencies and system failure probabilities developed from the precursors themselves are used when possible.

Rank precursors as to significance and identify attributes of more significant events.

Review of LERs for Potential Precursors

All 1984-87 LERs were reviewed by two engineers for potential precursors. Events selected during this review were then subjected to a detailed analysis. Events selected for detailed review included:

- core-damage initiators (including LOFWs, LOOPs, and small-break LOCAs);
- all events in which reactor trip was demanded;
- all support system failures, including failures in cooling water systems, instrument air, instrumentation and control, and electric power systems;
- any event where two or more failures occurred;
- any event or operating condition that was not predicted or proceeded differently for the plant design basis; and
- any event that, based on the reviewers' experience, could have resulted in or significantly affected a chain of events leading to potential severe core damage.

For 1988-89, LERs screened as Category 2 by AEOD and all reactor trips were reviewed for precursors. This reduced the number of LERs requiring review by 75% and allowed for additional detailed review and documentation effort. However, the possibility exists that some potential precursors were not identified in Category 2 events.

Review of LERs for Potential Precursors (cont.)

Use of the SCSS data base to screen LERs for potential precursors has been explored in the ASP program. A computerized screening approach was developed which identified a subset of 25% of LERs which contained almost all precursors which had been identified in 1984-89. Screening manpower requirements were reduced by 40-50% compared to manual reviews.

Efforts to further confirm the usefulness of SCSS in identifying precursors are currently underway. This effort involves a manual review of all 1990 LERs.

For 1990, the SCSS data base was screened to identify potential precursors. These events were reviewed along with AEOD Category 2 events. All events finally selected as precursors were identified using the computerized screening approach.

Review of LERs for Precursors: Detailed Review

The detailed review of selected events considers the immediate impact of an initiating event or the potential impact of equipment failures or operator errors on readiness of systems in the plant for mitigation of off-normal and accident conditions. Three general scenarios are considered:

- If the event or failure was immediately detectable and occurred while the plant was at power, then the event is evaluated according to the likelihood that it and the ensuing plant response could lead to severe core damage;
- If the event or failure had no immediate effect on plant operation (i.e. if no initiating event occurred), then the review considers whether the plant would require the failed items for mitigation of potential severe core-damage sequences given a postulated initiating event during the failure period; and
- If the event or failure occurs while the plant was not at power, then the event is evaluated according to whether it could have occurred while at power or at hot shutdown immediately following power operation or if it could have only occurred at cold shutdown conditions. If an event could have occurred at power, it is typically evaluated under that condition.

Four Sets of Attributes Are Common To ASP Events

Events are selected and documented as accident sequence precursors if they include one of the following attributes:

- a core-damage initiator (such as a LOOP, small steam-like break, or small-break LOCA);
- a failure of a system (all trains of a multiple-train system) required to mitigate the consequences of a core-damage initiator;
- degradation in more than one system required to mitigate the consequences of a core-damage initiator; or
- reactor trips and losses of feedwater with a degraded mitigating system (1984 and following),

and if the estimated conditional probability of subsequent severe core damage $\geq 10^{-6}$ (1987 and following). Documentation includes 2-3 pages of descriptive material plus supporting tables, graphs, diagrams, and computer output sheets.

Failures in containment-related systems (total failures and multiple degrades) and other interesting events are also documented.

Precursor Modeling Approach

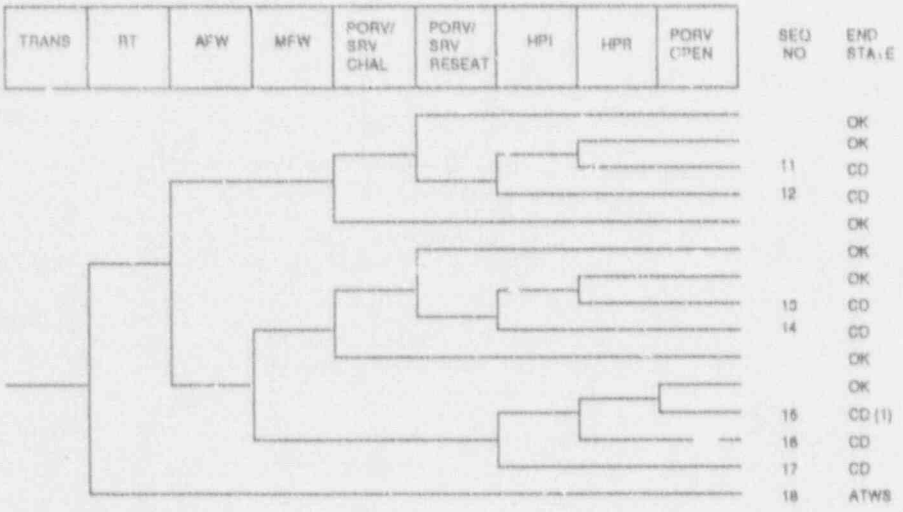
U.S. LWRs have been divided into eight plant classes -- five for PWRs and three for BWRs. The classes are defined based on the use of similar systems for accident sequence mitigation and similar response, on a system level, to initiating events.

Transient, loss-of-offsite power and small-break LOCA event trees were developed for each plant class. Each event tree addresses both safety-related and non-safety systems which can be used to mitigate off-normal events. Using such trees, the impact of system-level operation on individual plant classes can be distinguished.

Two undesired end states are included in the event trees:

- core damage (inadequate core cooling); and
- ATWS (failure to scram).

Example Event Tree Model



(1) OK for Class D

PWR Classes B and D Nonspecific Reactor Trip

Estimation of System-Level Failures

When adequate precursor information exists, system-level failure-on-demand probabilities are estimated from the precursors themselves by assigning a failure to recover (restore) likelihood to each failure, summing these likelihoods, and dividing by the estimated number of demands:

$$p(\text{system}) = \frac{\sum_{i}^{\text{observed failures on demand}} p_i(\text{failure to recover})}{\text{total demands in observation period}}$$

Table 1. System Nonrecovery Estimation

Recovery Class	Description	Likelihood of failing to recover from event [a]
R1	Failure did not appear to be recoverable in required period, either from control room or at failed equipment	1.00
R2	Failure appeared recoverable in required period at failed equipment, and equipment was accessible; recovery from control room did not appear possible	0.34
R3	Failure appeared recoverable in required period from control room, but recovery was not routine or involved substantial stress	0.12
R4	Failure appeared recoverable in required period from control room and was considered routine or procedurally based.	0.04

[a] These values are used for consistency of analysis. The actual likelihood of failing to recover from an event at a particular plant is difficult to assess and may vary substantially from the values listed above.

Conditional Probability of Severe Core Damage

Individual precursors are ranked as to significance by estimating a conditional probability of subsequent core damage given the failures observed during the event.

Failures identified during the review of each precursor are mapped onto the plant-class event trees which are then used to estimate a conditional probability of subsequent core damage, given the precursor.

In this estimation method, the probability of a system failing given that it was observed successful or not challenged is assumed equal to the failure on demand probability for the system, while the probability of a system failing given that it was observed failed is assumed equal to the likelihood of not successfully restoring the system to operation (non-recovery likelihood).

The conditional probability is a measure of the residual protection against core damage which existed during the event, and is a measure of precursor significance.

Precursor Calculational Process

1. Event sequences requiring calculation.

   If an initiating event occurs as part of a precursor (i.e., the precursor consists of an initiating event plus possible additional failures), then use the event tree associated with that initiator; otherwise, use all event trees impacted by the observed unavailability.

2. Initiating event probability.

   If an initiating event occurs as part of a precursor, then the initiator probability used in the calculation is the probability of failing to recover from the observed initiating event (i.e., the numeric value of the recovery class for the event).

   If an initiating event does not occur as part of a precursor, then the probability used for the initiating event is developed assuming a constant hazard rate. Event durations (the period of time during which the failure existed) are based on information included in the event report, if provided. If the event is discovered during testing, then one-half of the test period (15 days for a typical 30-day test interval) is assumed, unless a specific failure duration is identified.

Precursor Calculational Process (cont.)

3. Branch probability estimation.

   For event tree branches for which no failed or degraded condition is observed, a probability equal to the estimated branch failure probability is assigned.

   For event tree branches associated with a failed system, a probability equal to the numeric value associated with the recovery class is assigned.

   For event tree branches that include a degraded system (i.e., a system that still meets minimum operability requirements but with reduced or no redundancy), the estimated failure probability is modified to reflect the loss of redundancy, but the nominal non-recovery probability is not modified.

4. Conditional probability estimation.

   For unavailabilities, a differential measure is calculated by subtracting the nominal risk over the unavailability period from the conditional probability calculated using the modified event trees.

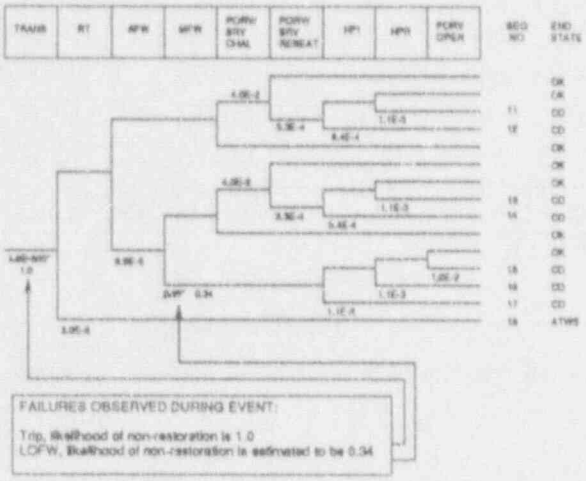
   For initiators, the nominal risk over the mitigation period is not subtracted since it is typically much smaller than the conditional probability calculated with an initiator probability of 1.0.

Precursor Calculational Process (cont.)

5. Support system unavailabilities.

   Systems or trains rendered unavailable as a result of support system failures are modeled recognizing that, as long as the affected support system remains failed, all impacted systems (or trains) are unavailable; but if the support system is recovered, all the affected systems are recovered. This can be modeled through multiple calculations which address support system failure and success. Calculated core damage probabilities for each case are normalized based on the likelihood of recovering the support system.

Example Transient Calculation



Postulated Event: Trip and Loss of Feedwater

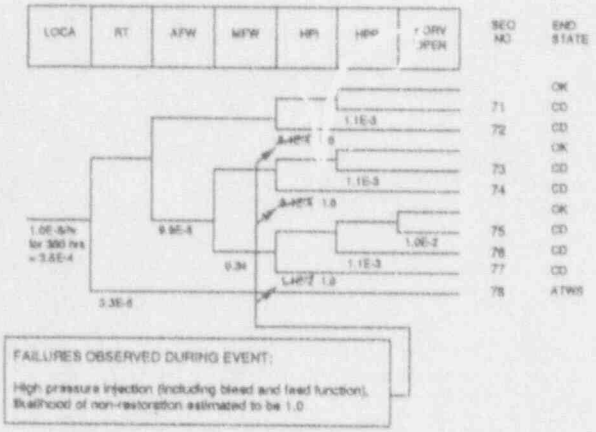
Likelihood of not recovering from trip = 1; likelihood of not recovering main feedwater estimated to be 0.34. No other failures observed during mitigation.

p(core damage) = p[seq. 11] + p[seq. 12] + . . . + p[seq. 17]
= 7.7×10^{-7}

p(ATWS) = p[seq. 18]
= 3.0×10^{-5}

Note: With the exception of relief valve challenge, failure probabilities are indicated.

Example Unavailability Calculation



Postulated event: unavailability of High Pressure Injection for 1/2 month. Likelihood of non-restoration estimated to be 1.0.

Probability of non-recoverable Small-Break LOCA in 360 hr period = 3.6E-4. Conditional probability of core damage given unavailability of HPI = 1.0.

p(core damage) = 3.6E-4 · nominal risk for same time period (7.0E-7) = 3.6E-4

Note: A complete analysis of this event would require postulated transients and LOOPs to be addressed as well.

Some Outstanding Issues

ASP data base is not totally consistent from year to year.

- Event tree models used for core damage calculations have changed from 1984 to 1990.
- Screening criteria for selected candidate events has changed from 1984-1990.

These inconsistencies can be eliminated without extensive effort for 1984 and later events.

Improved event tree models are being developed for NRR by SAIC. These models are based on the ASP models, but reflect NUREG-1150 insights to a greater degree than the current ASP models, include additional initiating events, and address alternate long-term cooling strategies. These models will be usable in the ASP program once they are completed.

Improvements need to be made to the process of estimating non-recovery likelihoods.

The potential use of detailed PRAs to analyze operational events needs to be explored.

Potential issues in the use of precursor conditional probabilities to estimate a retrospective frequency need to be explored.

APPENDIX G

View Graphs

for

Methods for Identifying Risk Significant Trends

Gareth W. Parry

METHODS FOR IDENTIFYING RISK SIGNIFICANT TRENDS

presented by

Gareth W. Parry
HALLIBURTON NUS Environmental Corporation

at

Workshop on the Use of PRA Methodology for the Analysis of Reactor Events and Operational Data
Annapolis, Maryland

HALLIBURTON NUS Environmental Corporation

DISCUSSION TOPICS

- **Given an Event Data Base (e.g., LER) and a Component Data Base (e.g., NPRDS), and a PRA Model for each plant, discuss:**
  - methods for screening data to identify those data elements that are risk or safety significant,
  - methods for analyzing that reduced set to identify trends,
  - data needs to provide meaningful results.

HALLIBURTON NUS Environmental Corporation

USE OF PRA MODELS

- **As a general rule, PRAs are an excellent filter for screening risk-important events**
  - importance measures
  - instantaneous risk measure (failures, initiating events)
  - time averaged risk increase/decrease (unavailabilities)
- **However,**
  - PRAs do not usually address phases of operation other than full power
  - do not model all components
  - do not model causes of failure

HALLIBURTON NUS Environmental Corporation

USE OF PRA MODELS (Continued)

- **PRA models are structurally static, therefore, trends are identified through parameter value changes (e.g., initiating event frequencies, component unavailabilities, human error probabilities)**
- **PRA models often based on specific assumptions. Different assumptions by different analysts can influence the screening for risk importance (e.g., assumptions about room cooling).**
- **PRA models are generally developed down to the level of failure mode. For comparison with the PRA model, the events have to be translated into their impact on the components of the model.**

HALLIBURTON NUS Environmental Corporation

SCREENING CRITERIA

- **Include degraded states as well as (PRA-Based) failures**
  - Degraded states may be indicative of underlying problems or trends
- **Screen events against all plant PRAs or just that at which it occurred?**

HALLIBURTON NUS Environmental Corporation

ANALYSIS OF SCREENED DATA

- **In its most basic form, data is numbers of events affecting components and/or systems, and a measure of opportunity. Therefore, analysis primarily focuses on rates.**
- **Key issues:**
  - grouping of data
  - establishing hypotheses

HALLIBURTON NUS Environmental Corporation

GROUPING OR POOLING DATA

- **Events related to specific components in a specific plant are rare, therefore, statistical fluctuations can mask trends.**
- **Increasing sample size increases signal to noise ratio**
- **Increasing sample size makes sense for:**
  - generic trends (e.g., aging),
  - underlying effects which cut across component types.

HALLIBURTON NUS Environmental Corporation

ESTABLISHING HYPOTHESES

- **To analyze data statistically, it is necessary to have some mental model of effects to be analyzed. The hypotheses give guidance for grouping data.**
- **Examples:**
  - Exploring aging - time origin is taken as start of life, plant data grouped by year since start of life.
  - Exploring impact of change in regulation - time origin is shifted to date of implementation.
  - Exploring impact of maintenance policy change at a plant - all components affected may be regarded as the pool of data.
  - Exploring impact of change of a specific piece of equipment - only that component's data is valid.

HALLIBURTON NUS Environmental Corporation

DATA NEEDS

- Emphasis on recent developments in PRA methodology has been explicit consideration of causes as a means of identifying potential fixes;
  - e.g., common cause failure analysis and human reliability
- Insights into what data are required to support these analyses highlight the need for a detailed description of the events including all contributing causes and influence factors.

HALLIBURTON NUS Environmental Corporation

THE CAUSE-DEFENSE PICTURE OF CCFs

- NUREG/CR-5460 stresses the importance of understanding the chain of events that led to failure:
  - Trigger events
  - Conditioning events
- The role of Defenses, and how they are defeated is crucial
- Root Cause related to identification of defense against recurrence.

HALLIBURTON NUS Environmental Corporation

INFORMATION REQUIREMENTS

- **Engineering Data**
  - Description of component, its boundaries, operating and failure modes
- **General Requirements for Reliability Parameters**
  - Operational history, exposure, event reports
  - For each event an assessment of its impact
- **CCF Requirements**
  - Correlation of event reports for redundant components
  - Description of the causal chain leading to failure
  - Method of discovery
  - Corrective action
  - Inspection/Testing/Maintenance Practices

HALLIBURTON NUS Environmental Corporation

APPENDIX H

View Graphs

for

"Approaches for Analyzing Data to Address Generic Issues Related to Common Cause Failures, Human Factors, and Systems Interactions"

Ali Mosleh

APPROACHES FOR ANALYZING DATA TO ADDRESS GENERIC ISSUES RELATED TO COMMON CAUSE FAILURES, HUMAN FACTORS, AND SYSTEMS INTERACTIONS

Ali Mosleh

Materials and Nuclear Engineering Department
University of Maryland, College Park

Presented at

Workshop on the Use of PRA Methodology for the Analysis of Reactor Events and Operational Data

Annapolis, Jan 28-29, 1992

GENERAL OBSERVATIONS

- TO IMPROVE THE QUALITY OF THE ACCURACY OF PRA MODELS OPERATIONAL DATA MUST BE USED BOTH QUALITATIVELY AND QUANTITATIVELY
- EQUALLY IMPORTANT BUT MUCH LESS ACKNOWLEDGED IS THE NEED FOR AN UNDERLYING MODEL TO GUIDE DATA COLLECTION AND ANALYSIS
- THESE TWO PROCESSES OUGHT TO BE INTERACTIVE AND ITERATIVE LEADING TO AN EVOLUTIONARY IMPROVEMENT IN MODELS AND DATA

COMMON CAUSE FAILURE ANALYSIS DATA NEEDS

- EFFECTIVE USE OF CURRENT MODELS REQUIRE
  - MORE ACCURATE DESCRIPTION OF THE EVENTS IN TERMS OF CAUSES AND IMPACT OF THE EVENT
  - LEVEL OF REDUNDANCY
  - SUCCESS DATA
- IMPROVED MODELS NEED (AS A MINIMUM) INFORMATION ON
  - COUPLING FACTOR(S)
  - BARRIERS AND DEFENSES BOTH AGAINST THE CAUSE AND THE COUPLING
  - FAILURE TIMES
- FUTURE MODELS WILL NEED, IN ADDITION TO THE ABOVE, INFORMATION ON PHYSICAL NATURE OF THE ROOT CAUSE AND COUPLING FACTOR OF THE EVENTS

SOME FACTS ABOUT COMMON CAUSE FAILURE EVENTS

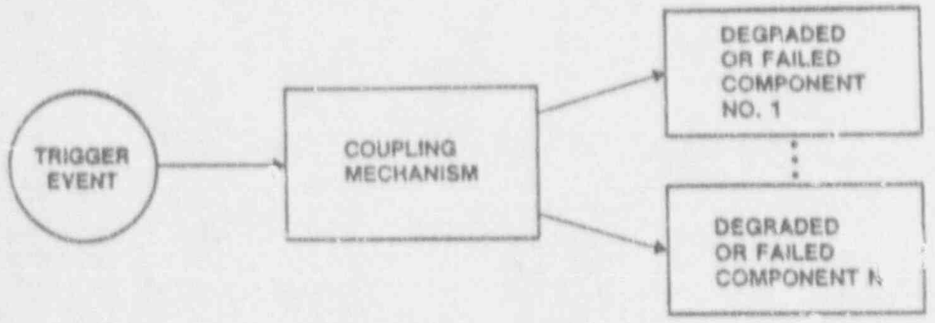
- CCF EVENTS ARE VERY RARE. A TWO-UNIT PLANT WITH MORE THAN 22 YEARS OF OPERATIONAL DATA HAS ONLY EXPERIENCED 6 CCFs WHICH IS ABOUT 5% OF ALL FAILURES EXPERIENCED. OUT OF MORE THAN 4000 LERs REVIEWED ONLY ABOUT 150 WERE CCFs OF THE TYPE MODELED IN PRAs (POWER OPERATION ONLY)
- REVIEW OF THE CCF DATA INDICATES COMMON CHARACTERISTICS WITH GENERIC IMPLICATIONS PARTICULARLY WITH RESPECT TO COUPLING FACTORS AND DEFENSE STRATEGIES.

IMPLICATIONS FOR MODELING AND DATA ANALYSIS

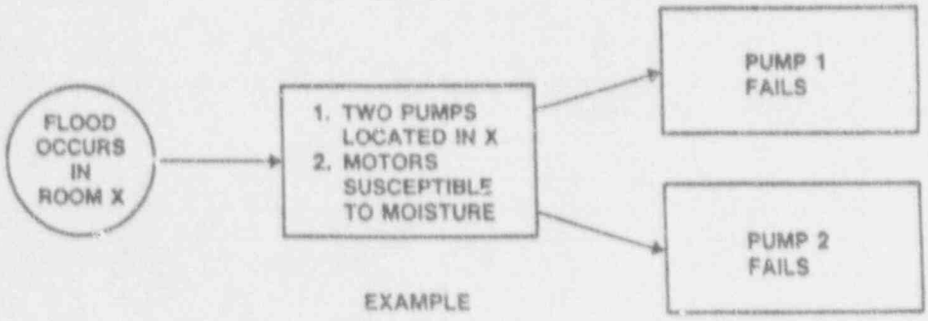
- PLANT-SPECIFIC PRAs MUST CONSIDER INDUSTRY (GENERIC) EXPERIENCE FOR COMPLETENESS OF CCF MODELING AND REALISTIC ASSESSMENT OF PROBABILITIES

- DATA FROM VARIOUS PLANTS NEED TO BE ANALYZED ACCORDING TO A COMPREHENSIVE CLASSIFICATION SYSTEM IN ORDER GAIN GENERIC INSIGHTS INTO THE UNDERLYING CAUSES OF COMMON CAUSE FAILURES. CURRENT DATA REPORTING SYSTEMS (INCLUDING LER AND NPRDS) LACK ADEQUATE RECORDING AND REPORTING GUIDELINES FOR CCF EVENTS.

PHYSICAL MODEL OF A COMMON CAUSE EVENT



MODEL



EXAMPLE

CCF CLASSIFICATION

* CCF TYPES

CCF TYPE I : Components of a system fail almost immediately, given a CCF Shock.

CCF TYPE II: Components of a system may fail after some time, given a CCF Shock. Components may or may not fail at the same time.

* SPECIFIC CASES

CASE A: The coupling factor couples components in a random fashion so that the components fail conditionally independently.

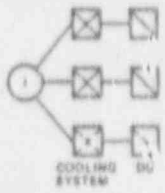
CASE B: The coupling factor acts on the components in a dependent fashion.

A TYPICAL TIME-DELAY FAILURE EVENT

PILGRIM - MAY 1974

Four salt service water system pumps became or were made inoperable during a 5 day period. Pump "D" was removed from service because it was making a loud and unusual noise. Upon disassembly, it was observed that the key of the motor shaft was sheared at the key way. The same kind of faults were also observed for other three pumps.

EXAMPLE OF IMPACT VECTOR ASSESSMENT WITH MULTIPLE INTERPRETATION OF EVENT

Plant (Date)	Status	Event Description	Cause-Effect Diagram
Maine Yankee (August 1977)	Power	Two diesel generators failed to run due to plugged radiator. The third unit radiator was also plugged.	

(a) Event Classification

Component Group Size	Hypothesis	Probability	F_0	F_1	F_2	F_3	Shock Type	Fault Mode
3	I_1	0.9	0	0	1	0	Nonlethal (N)	Failure during Operation
	I_2	0.1						
	Average Impact Vector (I)							

(b) Multiple Hypothesis Impact Vector Assessment

ISSUES RELATED TO HUMAN RELIABILITY MODELS AND DATA

- HUMAN RELIABILITY ESTIMATES AS APPLIED TO NUCLEAR POWER PLANT PRAs ARE ALMOST COMPLETELY BASED ON JUDGEMENT. EVEN IN THOSE CASES WHERE DATA COLLECTION HAS BEEN ATTEMPTED, MODELS WHICH ARE NOT VALIDATED NOR SUPPORTED BY A THEORETICAL OR EMPIRICAL FOUNDATION DENOMINATE THE RESULTS

- WITH THE EXCEPTION OF A RECENTLY LUNCHED AEOD PROGRAM THERE HAS BEEN NO SYSTEMATIC EFFORT TO COMPILE AND ANALYZE ACTUAL OPERATING EXPERIENCE FROM HUMAN PERFORMANCE POINT OF VIEW

- GENERALLY SPEAKING CURRENT MODELS DO NOT REFLECT ACTUAL OPERATING EXPERIENCE. EVEN QUALITATIVE INSIGHTS FROM THE LIMITED OPERATIONAL DATA HAVE NOT BEEN USED SYSTEMATICALLY IN THE MODELS

EXAMPLES OF INSIGHTS FROM EVENT REVIEWS PERFORMED UNDER AEOD PROGRAM

- O EOP INADEQUACY WITH RESPECT TO HNDLING PARTIAL FAILURES OF SYSTEMS
- O DIFFERENCE BETWEEN ACTUAL PLANT RESPONSE AND RESPONSE OF SIMULATORS USED TO TRAIN THE OPERATING CREW
- O CREW ERROR IN ASSESSING THE NATURE OF PLANT UPSET AND RECOVERY ACTIONS AS A RESULT OF COMMON CAUSE UNAVAILABILITY OF REDUNDANT INSTRUMENTATION

SOME ACHIEVABLE GOALS

- O QUANTITATIVE DATA FOR ERROR PROBABILITY ESTIMATES IS DIFFICULT (AT LEAST FOR DIRECT ESTIMATION) SINCE SUCCESS DATA IS VERY DIFFICULT TO OBTAIN. NEVERTHELESS SOME CONSIDERATION SHOULD BE GIVEN TO IDENTIFYING POSSIBLE APPROACHES FOR COLLECTING SUCCESS DATA. THIS MIGHT BE EASIER IN THE CASE OF OPERATOR RESPONSE TO INITIATING EVENTS.
- O EFFORTS IN THE AREA OF COLLECTING , ANALYZING AND CLASSIFYING HUMAN PERFORMANCE DATA SHOULD BE EXPANDED. THE DIRECT BENEFIT WILL BE IN GAINING INSIGHTS INTO CAUSES AND MODES OF HUMAN ERRORS. SUCH INSIGHTS CAN BE USED TO IMPROVE PLANT SAFETY, SOMETIMES WITH MINOR CHANGES IN PLANT OR OPERATING PRACTICES AND PROCEDURES. THEY CAN ALSO PROVIDE MUCH NEEDED "REAL LIFE" INPUT TO THE HUMAN RELIABILITY MODEL BUILDING ACTIVITIES.

APPENDIX I

View Graphs

for

"Industry Risk Profiles: Do We Need More Modeling?"

George Apostolakis

INDUSTRY RISK PROFILES: DO WE NEED MORE MODELING?

by

George Apostolakis

Mechanical, Aerospace & Nuclear Engineering Department
38-137 Engineering IV
University of California
Los Angeles, CA 90024-1597

Tel: (310) 825-1300
Fax: (310) 206-2302

Presented at the

Workshop on the Use of PRA Methodology for the Analysis of Reactor Events and Operational Data

Annapolis, Maryland
January 29-30, 1992

CONCLUSIONS

- Operational experience is of limited value unless it is interpreted through validated models.
- Drawing generic conclusions from operational experience makes the need for models more urgent.
- Developing validated models would require significant resources.

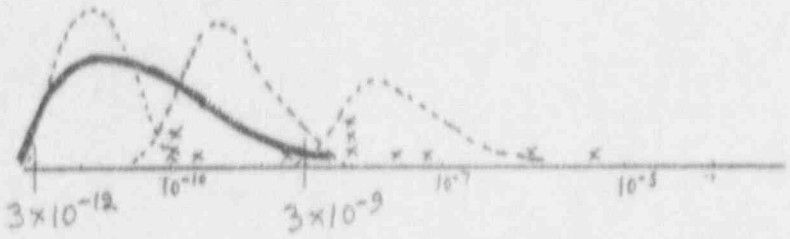
REACTOR SAFETY STUDY

"THE RELIABILITY RESULTS WHICH WERE COMPUTED WERE TO APPLY TO A POPULATION OF REACTOR PLANTS (100) AND HENCE IT WAS DESIRED TO MODEL THE COMPONENT FAILURE VARIABILITY FROM PLANT TO PLANT."

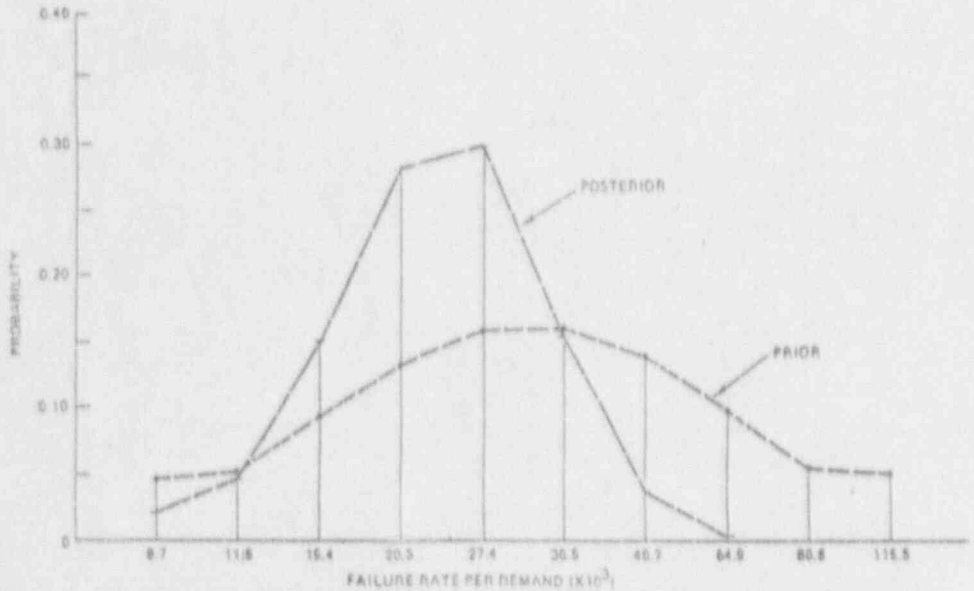
SOURCES: HANDBOOKS, REPORTS, OPERATING EXPERIENCE, DEPARTMENT OF DEFENSE, NASA, ET AL.

ORDER OF MAGNITUDE ACCURACY

ASSESSED RANGE ⇒ LOG NORMAL DISTRIBUTION



per hour
per pipe section



Prior and Posterior Histograms for Diesel Generators — Failure to Start

MODEL AND PARAMETER UNCERTAINTIES

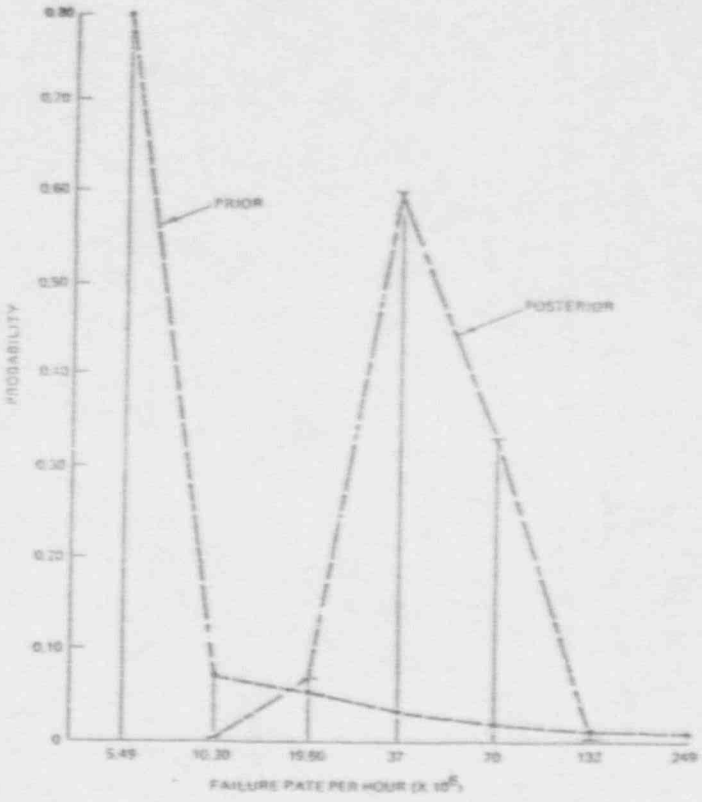
$$\bar{h}(A|H) = \sum_{i=1}^{n}\left[\int h_i(A|\phi_i, M_i, H)\,\pi_i(\phi_i|M_i, H)d\phi_i\right] p(M_i|H)$$

UPDATED PROBABILITIES

$$p(M_i|E) = \frac{\int h_i(E|\phi_i, M_i)\pi_i(\phi_i|M_i)d\phi_i}{\sum_{i=1}^{n}\left[\int \pi(\phi_i|M_i)h_i(E|\phi_i, M_i)d\phi_i\right]p(M_i)}\, p(M_i)$$

and

$$\pi_i(\phi_i|M_i, E) = \frac{h_i(E|\phi_i, M_i)}{\int \pi_i(\phi_i|M_i)h_i(E|\phi_i, M_i)d\phi_i}\,\pi_i(\phi_i|M_i)$$



Revised Prior and Posterior Histograms for Pressure Sensors

$$E = \{t_1, t_2, \ldots, t_n\}$$

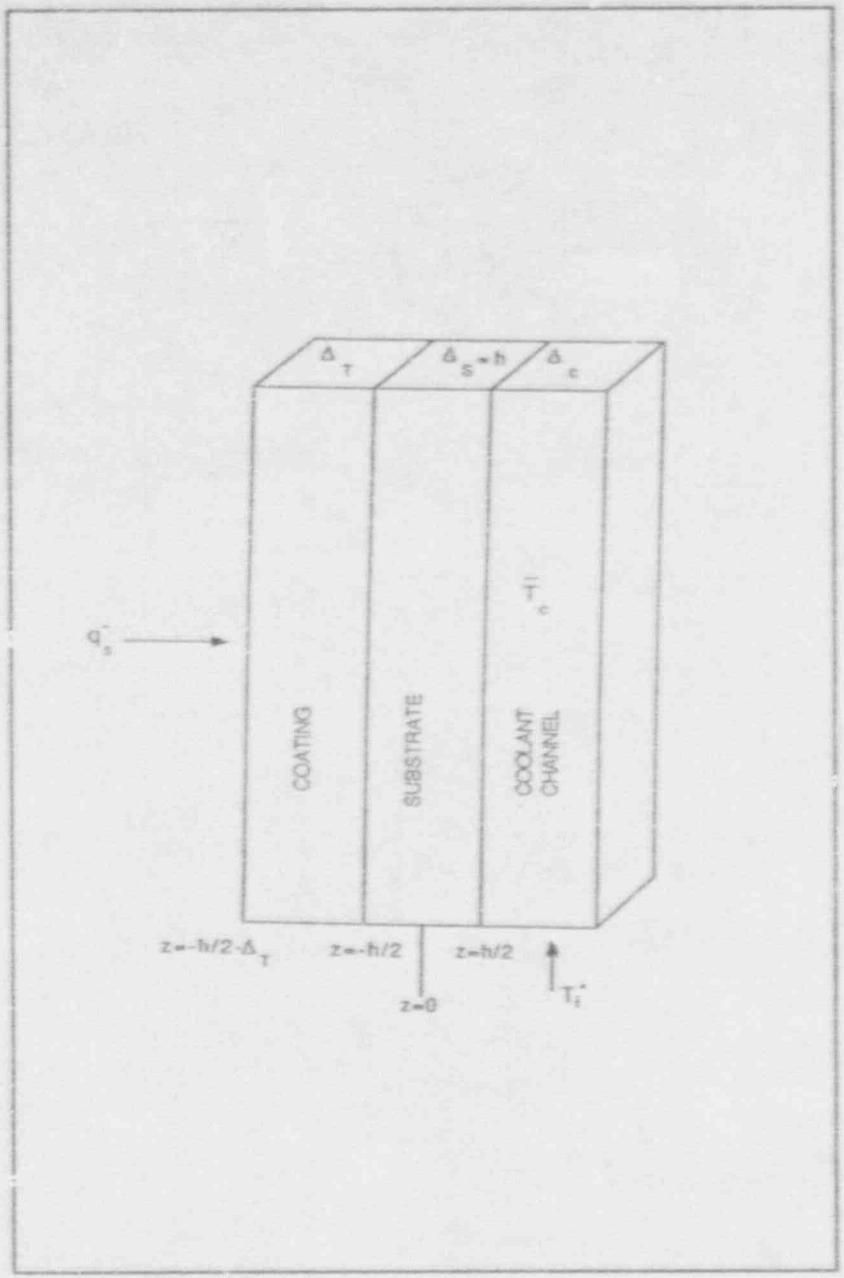
$$\pi_1(\lambda|\tau) = \frac{\lambda^N \exp(-\lambda T)\, \pi_0(\lambda)}{\int_0^\infty \lambda^N \exp(-\lambda T)\, \pi_0(\lambda)\, d\lambda}$$

$$T = \sum_{j=1}^{N} \tau_j$$

$$\pi_1(\lambda|E) = \int_0^\infty d\tau_1 \cdots \int_0^\infty d\tau_N\, \pi_1(\lambda|\tau) \prod_{j=1}^{N} p_j(\tau_j|E_j)$$

UNCERTAIN OR DEBATABLE EVIDENCE

- FIRE DETECTION
- FIRE FREQUENCY
- RECTIFIABILITY



DEBATABLE STATISTICAL EVIDENCE

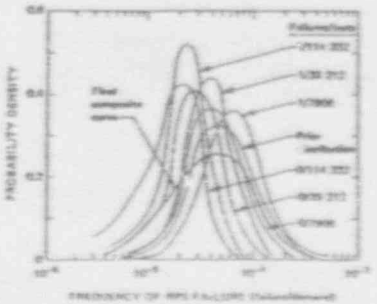
$E_i = [K_i \text{ EVENTS IN } N_i \text{ TRIALS}]$, $\quad i = 1 \ldots N$

$$\pi_c(x) = \sum_{i=1}^{N} \pi(x|E_i) P_i$$

Numbers of Screen Trials and Failures for Calculation of Posterior Curves

Screen	Failures r	Trials n
NRC	1	7 908
"	0	7 908
EPRI—not counting	1	39 212
saved data	0	39 212
EPRI—counting	1	114 212
saved data	0	114 372

"This case was added to obtain a complete view of possible posterior curves.



Final component probability curves for screen failure rate.

FAILURE MODELS

1. THERMAL MODELS TO CALCULATE TEMPERATURE DISTRIBUTIONS THROUGH A COMPONENT DURING NORMAL AND TRANSIENT CONDITIONS;

2. STRESS-STRAIN MODELS INCORPORATING THERMAL AND IRRADIATION CREEP, AND SWELLING;

3. OTHER.

$$R(t|\underline{\phi}) = \begin{cases} e^{-\lambda_c t} \sum_{k=0}^{\min(FC(n),\infty)} \frac{(\lambda_{nc} t)^k e^{-\lambda_{nc} t}}{k!} & , t > 0 \\ 1 & , t = 0 \end{cases}$$

$$R(t|\underline{\phi}) = e^{-\lambda_c t}\left[1 - P(1 + \min(FC(t)); \lambda_{nc} t)\right]$$

"When both steam generators are dry, the procedure requires the initiation of make-up/high pressure injection (MU/HPI) cooling, or what is called the "feed-and-bleed" method for decay heat removal... When the hot-leg temperature reached 591° F (normal post-trip temperature is about 550° F), the secondary-side operator recommended to the shift supervisor that MU/HPI cooling be initiated. At about the same time, the operations superintendent told the shift supervisor in a telephone discussion that if an auxiliary feedwater pump was not providing cooling to one steam generator within one minute, to prepare for MU/HPI cooling. However, the shift supervisor did not initiate MU/HPI cooling. He waited for the equipment operators to recover the auxiliary feedwater system.

The shift supervisor appreciated the economic consequences of initiating MU/HPI cooling. One operator described it as a drastic action... Despite his delay, the shift supervisor acknowledged having confidence in this mode of core cooling based on his simulator training; he would have initiated MU/HPI cooling if "it comes to that"."

"Loss of Main and Auxiliary Feedwater Event at the Davis-Besse Plant on June 9, 1985" NUREG-1154, July 1985.

- The shift supervisor's hesitation to initiate MU/HPI cooling is essentially treated as a non-event in NUREG/CR-4674.

- The emphasis is on component failures and operator errors (incorrect actuation of Steam and Feedwater Rupture Control System on low steam pressure instead of the desired low steam generator level)

"The proper method of manual actuation of the SFRCS buttons will be reviewed with all licensed operators. The switch layout is being modified to add additional demonstration of the situation buttons and to add actuation guards over the switches."

"Operator interviews indicated that the shift was fully aware of the core stations and were prepared to implement the bleed-and-feed" core cooling method if the auxiliary feedwater was not restored."

LER Text in NUREG/CR-4674, vol. 2, Dec. 1986

ORGANIZATION FACTORS RELEVANT TO SAFETY

Strategic Apex:
1. Goal Priority
2. Responsiveness
3. Safety vs. Bottom Line Orientation
4. Hardware vs. Human Relations Emphasis
5. Regulatory Relationships
6. Industry Competition
7. Public Opinion
8. Union-Management Relations
9. Board Nuclear Review Committee
10. Nuclear Safety Review Committee
11. Independent Safety Engineering Group
12. Onsite Review Organization
13. Formalization
14. Coordination/Integration
15. Cooperation
16. Interdependence
17. Centralization
18. Safety Culture
19. Long Range Plans

Inter-Departmental:
1. Agreement on Goal Priority
2. Ownership vs. Blaming others
3. Linkages with Contractors
4. Speed of Conflict Resolution
5. Formalization
6. Coordination/Integration
7. Cooperation
8. Interdependence

Ergonomic:
1. Engineering Design and [illegible] Support
2. Tolerance for Sub-Standard Equipment
3. Ineffective Trending
4. Method for Employees to Identify Potential Problems
5. General House Keeping

Decision-Making:
1. Procedural Clarity/Completeness
2. Procedural Updtes
3. Proactive vs Reactive
4. "At Right Level"
5. Methods for Setting Work Priorities
6. Updating Documentation and Drawings
7. Abuse of Priority Status
8. Management Support for Lower Level Problem Solving

Personnel:
1. Accountability

- Organizational culture refers to the value system of an organization.
- Plant policies may set priorities of operator actions long before emergencies.
- A fundamental management responsibility is the establishment of a safety culture governing the actions and interactions of all individuals and organizations engaged in activities related to nuclear power (IAEA INSAG).

BUT

Practical and validated models for NPP organizations are not available yet.

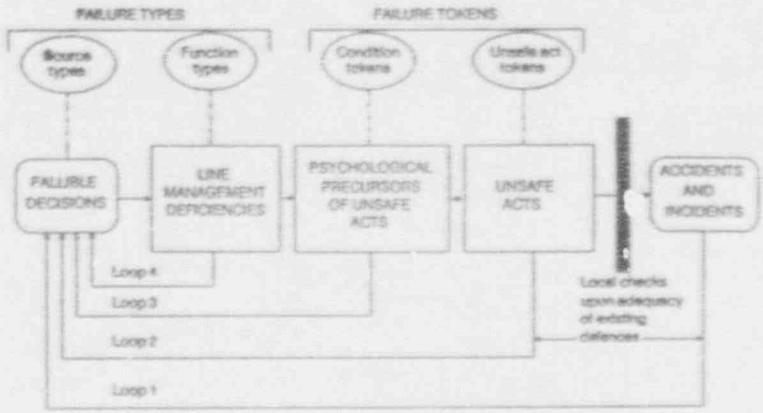


Figure 7.9. Feedback loops and indicators. The indicators are divided into two groups: *failure types* (relating to deficiencies in the managerial/organisational sectors) and *failure tokens* (relating to individual conditions and unsafe acts).

J. Reason, Human Error, Cambridge University Press, 1990.

2. Job Standards
3. Administrative Burdens
4. Disciplinary Systems
5. Incentive Systems
6. Promotion/Hiring Systems
7. Performance Evaluation Systems
8. Job Rotation
9. Training
10. Feedback Systems
11. Assessment of Contractor Capabilities
12. Supervisory Skills
13. Pay Equity
14. Recognition/Reward System
15. Overtime Policies
16. Timeliness of Key Replacements

Intra-Departmental:

1. Vertical Communication
2. "Right First Time"
3. Departmental Goals
4. Employee Input Mechanisms
5. Open Problem Solving
6. Management by Walking Around
7. Teamwork
8. Morale
9. Goal Priority
10. Shift Turnover Practices
11. Work Planning/Scheduling

Miscellaneous:

1. Root Cause Analysis
2. Effectiveness of Plant Onsite Review Committee
3. Performance Evaluation Programs (PEPs)
4. Deviation Event Reporting System
5. Performance Scheduling and Tracking Program
6. Surveillance Scheduling and Tracking Program
7. Inventory Control and Updating
8. Work Package Planning and Updating
9. Preventative Maintenance and Control
10. Quality Assurance Audits
11. Percentage of Managers Reporting Off Site
12. Clashing Cultures
    a. Engineers vs. Non-Engineers
    b. Nuclear Navy vs. Non-Nuclear Navy
    c. Employees vs. Contractors
13. Housekeeping/Documentation Procedures
14. Regulatory Orientation
15. System Wide Understanding
16. Deep Technical Knowledge

APPENDIX J

View Graphs

for

"Use of PRAs and IPEs for Event Risk Analysis"

Arthur C. Payne, Jr.

Use of PRAs and IPEs for Event Risk Analysis

Arthur C. Payne Jr.
Sandia National Laboratories

Presented to:
Workshop on the Use of PRA Methodology
for the Analysis of Reactor Events and Operational Data

January 29, 1992

What are our goals?

1. To be able to assure the public that nuclear power plants are being operated in a safe manner.

2. To develop improved techniques for identifying events that may compromise the predicted level of safety.

What Measure Do We Use to Evaluate the Significance of Possible Accidents?

1. The bottom line measure should be related to offsite risk to the public and environment from possible accidents.

2. These measures can be decomposed into several subsidiary measures:

    - frequency of core damage,
    - conditional probability of vessel breach,
    - conditional probability of containment failure,
    - magnitude of the source term, and
    - consequence to the public.

How Do We Identify Risk Significant Events?

1. Evaluation of past events, depending on the quality of the data.

2. Theoretical analysis techniques such as PRA, systems analysis, etc.

What do We Need in Order to Use PRAs/IPEs to Perform Event Evaluations and Operational Data Trending?

1. One needs a set of PRAs on all plants performed to a consistent level of detail and performed with the same goal in mind or
2. One needs a system that can account for differing levels of details and goals.

How Can We Design a System Using a Consistent Level of Detail?

1. Upgrade current system -
   a. Select a set of representative plants, incorporating detailed PRA models of these plants into ASP or construct a set of simplified plant models for each plant (ASEP results might be used to generate models or IPE/PRA models might be incorporated directly).
   b. Include models for every plant (Again ASEP or IPEs might be used as a bases).
   c. Include all accidents modeled.
2. Evaluate all other PRAs/IPEs to see if surrogate models represent each class of plants or if simplified models capture significant characteristics of plants.

How Can We Design a System Using a Consistent Level of Detail? (Concluded)

3. Upgrade models to include plant-to-plant variations in design if determined to significant.

4. Use the current ASP approach to evaluate events. If events are not represented, upgrade models.

How Can We Design a System to Account for Differing Levels of Details and Goals?

1. Determine the Theoretical Characteristics of Events.

   Examples:

   a. Frequency or probability.
   b. Number of components affected.
   c. Importance in model.
   d. Detectability of Failure.
   e. Diagnosabilty.
   f. Severity of Sequences generated from.
   g. Not thought of.
   h. Able to Analyze.
   i. Number of plants with precursor.
   j. Complexity may obscure accurate diagnosis.
   k. What if event occurred else where? Different effect in different plants or system.

How Can We Design a System to Account for Differing Levels of Details and Goals? (Continued)

2. Determine characteristics of events that could be detected by data analysis.

3. Examine the events that have occurred to see if any characteristics are missing and if you are detecting events with those characteristics.

4. List characteristics of event that should be identified by PRA/IPEs or assumptions that should limit the identification of events.

How Can We Design a System to Account for Differing Levels of Details and Goals? (Continued)

5. Examine PRAs/IPEs to see if events with the appropriate characteristics are being identified.

   List characteristics of IPEs and PRAs.

   Internal vs. External,
   Level of detail,
   Nomenclature,
   Thermal-Hydraulic code used,
   Support calculations performed,
   Uncertainty included,
   Conservative, realistic, non-conservative,
   Current,
   Scope - type of errors not included,
   Method

   What are assessed in PRAs?, what are missing?

   RVR, multiple tube rupture, reactivity, instrumentation, operator errors of commission, design and construction errors, low power, spent fuel pool.

How Can We Design a System to Account for Differing Levels of Details and Goals? (Continued)

6. Compare two sets of characteristics to see which each method misses.

7. Construct an AI program to classify the characteristics of events determined to be dominant at plants from PRA analysis, other analysis techniques, or data.

   Could also enter the assumptions/limitations used in the analyses or data gathering.

8. Enter the characteristics of data events or theoretical events and see if any characteristics match or assumptions are violated. If does not match, ask for any characteristic changes that would make a match.

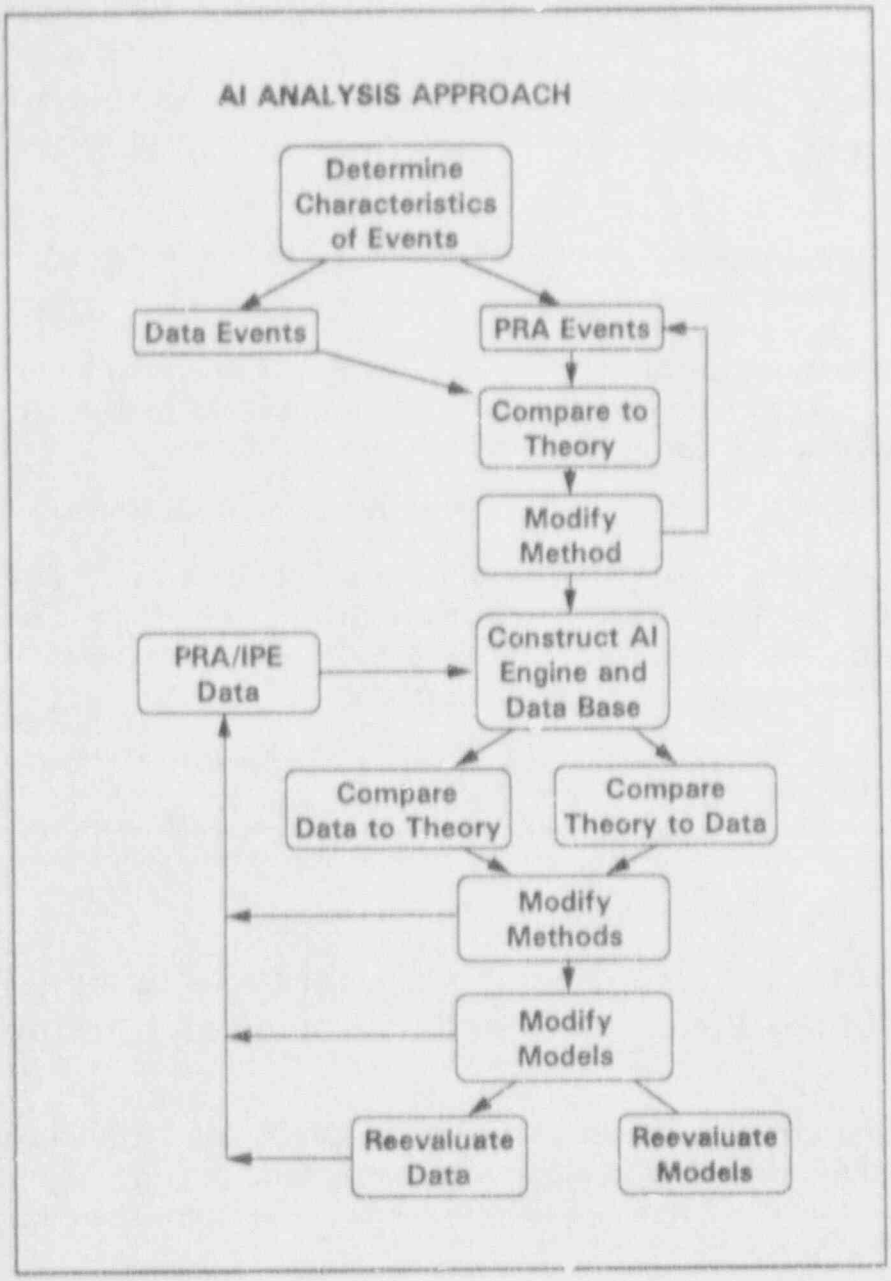
   The PRA, IPE, data base, and others could be tied to the AI program directly. Also plant design information could be included.

How Can We Design a System to Account for Differing Levels of Details and Goals? (Continued)

9. Go back and examine the data to determine if the events could have these characteristics or does the data reporting and analysis need to be changed. Similar consideration for PRA methodology.

10. Make a master matrix of all identified events from PRAs,IPEs, and data (etc.). Evaluate these events as to importance or if they have occurred in the data. Do data searches for ones which have not occurred yet but are important.

    Use matrix of events thought of or occurred, check off ones occurred, grade by significance, check trends in data, ccf, calculate frequencies and compare to theoretical frequencies.


AI ANALYSIS APPROACH
Determine Characteristics of Events
Data Events
PRA Events
Compare to Theory
Modify Method
PRA/IPE Data
Construct AI Engine and Data Base
Compare Data to Theory
Compare Theory to Data
Modify Methods
Modify Models
Reevaluate Data
Reevaluate Models

APPENDIX K

View Graphs

for

"Living PRA Concept"

Dennis Bley

LIVING PRA

by
Dr. Dennis C. Bley

presented at
WORKSHOP ON THE USE OF PRA METHODOLOGY FOR THE
ANALYSIS OF REACTOR EVENTS AND OPERATIONAL DATA

U.S. Nuclear Regulatory Commission
Office for Analysis of Operational Data

Annapolis, Maryland
January 29-30, 1992

PLG
ENGINEERS • APPLIED SCIENTISTS • MANAGEMENT CONSULTANTS
Newport Beach • CA
Washington • DC

"LIVING PRA" OVERVIEW

WHAT IS IT?

ITS USES

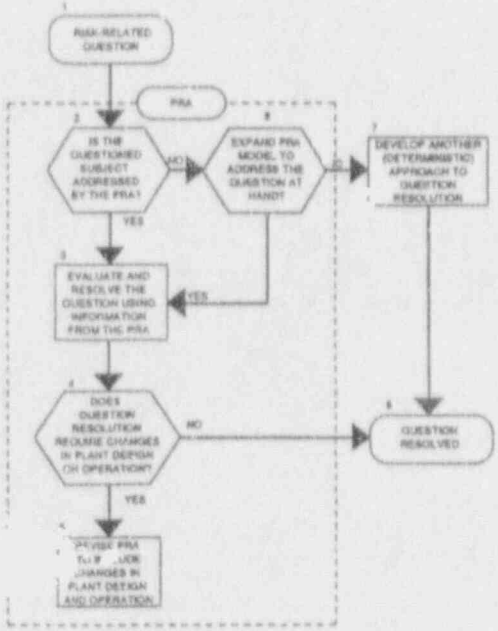
METHODS

DATA REQUIREMENTS

POTENTIAL FOR ADOPTION TO NRC USE FOR
RISK MONITORING AND EVENT ANALYSIS (ASP)

"LIVING PRA": WHAT IS IT?

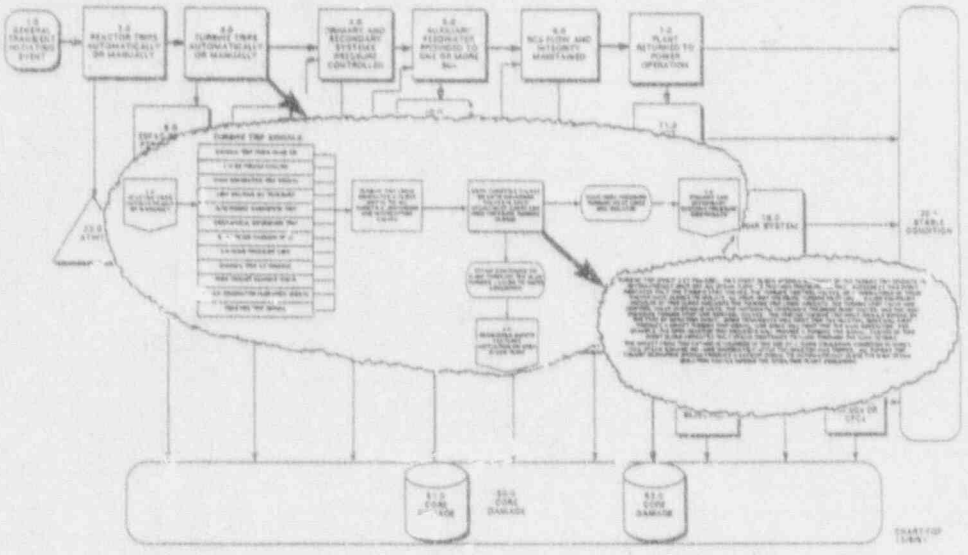
- CLICHÉ – ALL THINGS TO ALL PEOPLE
- A SUGGESTED SET OF DESIDERATA
  - FULL-SCOPE REALISTIC MODELS – MAINTAIN PERSPECTIVE
  - UP-TO-DATE DATA AND MODELS
  - CONSIDERATION OF UNCERTAINTY
  - ACCESSIBLE AND EASY TO USE
  - EASILY MODIFIED – ALLOW TESTING CHARGES
- A DAY-TO-DAY RISK MANAGEMENT TOOL



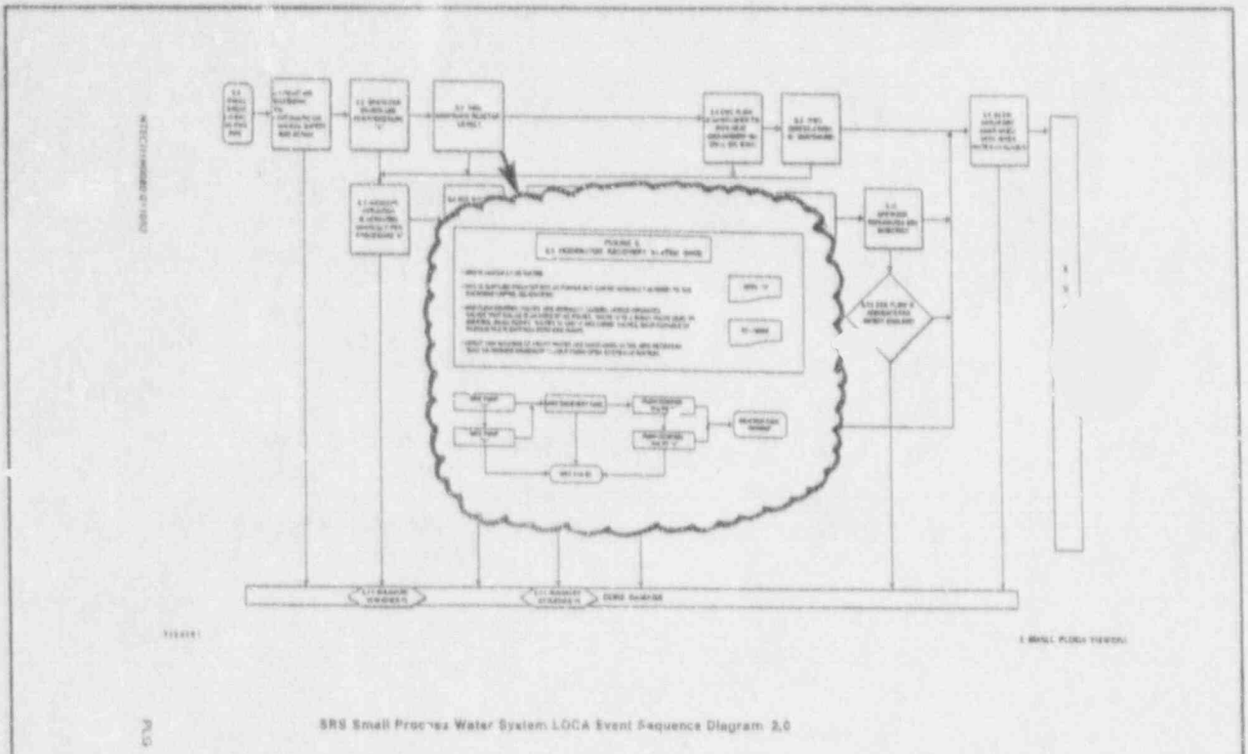
PRA Risk Management Application Process

"LIVING PRA"--ADDITIONAL INTERPRETATIONS

- ADAPTABLE, CAN ANSWER NEW ALTERNATIVE QUESTIONS
  - E.G., HOW CAN I FIND THE RISK FROM CONTAMINATION OF INSTRUMENT AIR?
- UPDATE FREQUENCY
  - AFTER MAJOR CHANGES
  - ANNUALLY, MONTHLY, DAILY
  - AFTER SIGNIFICANT INDUSTRY EVENTS
- ABILITY TO COMMUNICATE OUTSIDE THE PRA COMMUNITY

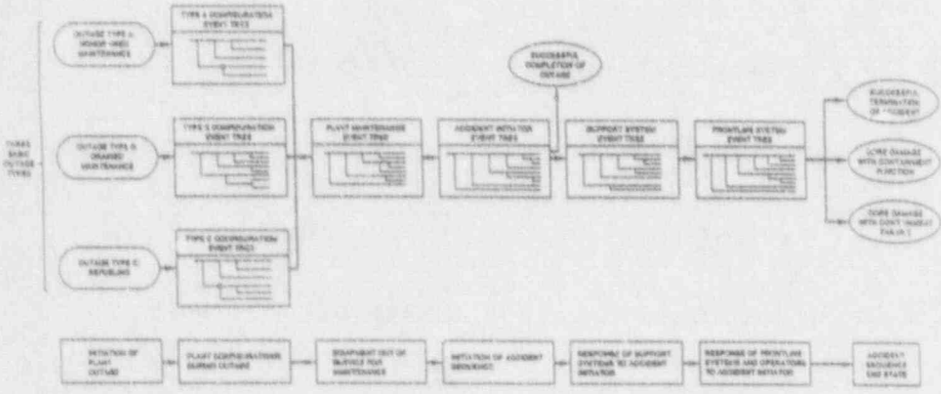


...mple Three-Dimensional Event Sequence Diagram



SRS Small Process Water System LOCA Event Sequence Diagram 3.0

EVENT TREE LINKING STRUCTURE FOR SHUTDOWN EVENTS PSA



"LIVING PRA"--POTENTIAL USES

- LOCATE WEAK POINTS IN PLANT
- SET PRIORITIES AMONG SAFETY PROBLEMS
- EVALUATE CHANGES TO EQUIPMENT AND PROCEDURES
- PLAN MAINTENANCE TO OPTIMIZE SAFETY AND PRODUCTION
- OPERATOR AND ENGINEER TRAINING

"LIVING PRA"--POTENTIAL USES

- DEVELOPMENT OF SAFETY CULTURE AND RISK AWARENESS
- OPTIMIZE TECHNICAL SPECIFICATIONS
- EVALUATE THE SIGNIFICANCE OF OPERATING EXPERIENCE
- SUPPORT ECONOMIC RISK EVALUATIONS
- SUPPORT EMERGENCY PLANNING AND RESPONSE

"LIVING PRA"--METHODS

- NEW CONCERNS FOR A "LIVING MODEL"
  - CONFIGURATION MANAGEMENT OF MODEL AND DATA
  - REVIEW OF DESIGN CHANGE PACKAGES
  - BAYESIAN UPDATE OF PREVIOUS DISTRIBUTIONS WITH NEW PLANT-SPECIFIC DATA
  - REVIEW OF INDUSTRY EVENTS

"LIVING PRA"--METHODS

- ARE NEW METHODS NEEDED TO SUPPORT SOME USES?
  - DISCRETE EVENT SIMULATION
  - DYNAMIC INTERACTION MODELS
  - NEW HUMAN COGNITIVE MODELS
  - FASTER ALGORITHMS

"LIVING PRA"--METHODS

- ARE NEW COMPUTER TOOLS NEEDED?
  - IMPROVED PERFORMANCE OR REPORTING
  - IMPROVED QUERY AND "WHAT IF?"
  - AI HYPERTEXT, OR GRAPHICS

"LIVING PRA"--DATA REQUIREMENTS

- UPDATE THE USUAL PRA DATA: FAILURE RATES, INITIATING EVENT FREQUENCY, MAINTENANCE FREQUENCY AND DURATION, COMMON CAUSE PARAMETERS
- OPERATING EXPERIENCE AS A CHECK ON PRA AS A CHECK ON THE RISK SIGNIFICANCE OF OPERATING EXPERIENCE
- HOW ABOUT OPERATING EXPERIENCE AS A CHECK ON HUMAN RELIABILITY ASSESSMENT?

OPERATING EXPERIENCE INSIGHTS FOR PRA

Type Experience	Example Information	Example Inferences
Actuarial Information	Operating Time Tests Actuations Failures, Trip Events Common Cause Failures Maintenance Actions Expert Knowledge	Initiating Event Frequency Failure Rate Maintenance Rate and Duration Common Cause Failure Rate System Unavailability Plant-to-Plant Variability
Actual Event Sequence Descriptions	Real Sequence of Events Timing of Events Interactions among Events Human Responses Rates of Processes Expert Experience	Correctness of Models Sequencing Interactions/Dependencies Validity of Success Criteria Time Available for Recovery Rate of Change of Parameters Uncertainty
Qualitative Descriptions of Performance	Environment Actual Extent of Damage Time of Under Adverse Conditions Effects of Recovery Actions Use of Procedures Psychological and Physical Stresses Expert Knowledge	Time to Functional Failure Does Failure Actually Occur New Failure Modes To Be Modeled Where Procedures Do/Do Not Work Time To Diagnose and To Carry Out Recovery Actions

"LIVING PRA"--POTENTIAL FOR ADAPTATION TO NRC USE FOR RISK MONITORING AND EVENT ANALYSIS (ASP)

- "RISK METER"
- PLANT-SPECIFIC EXAMINATION OF PRECURSOR EVENTS
  - OFFERS MANY IMPROVEMENTS
  - DO WE NEED NEW CRITERIA FOR PRECURSOR IDENTIFICATION?
- IDENTIFY WEAK SPOTS IN PRA
- INCENTIVE TO CROSS CATALOG PRECURSORS

SUMMARY

- LIVING PRA MUST BE
  - UP-TO-DATE
  - EASILY MODIFIED
  - ADAPTABLE
- LIVING PRA OFFERS
  - PLANT-SPECIFIC RISK-BASED REGULATORY DECISIONS
  - A DAY-TO-DAY RISK MANAGEMENT TOOL
  - RISK COMMUNICATION AND PERSPECTIVE

APPENDIX L

View Graphs

for

"Trending Plant Performance: Thoughts on Risk-Based Performance Indicators"

Joseph R. Fragola

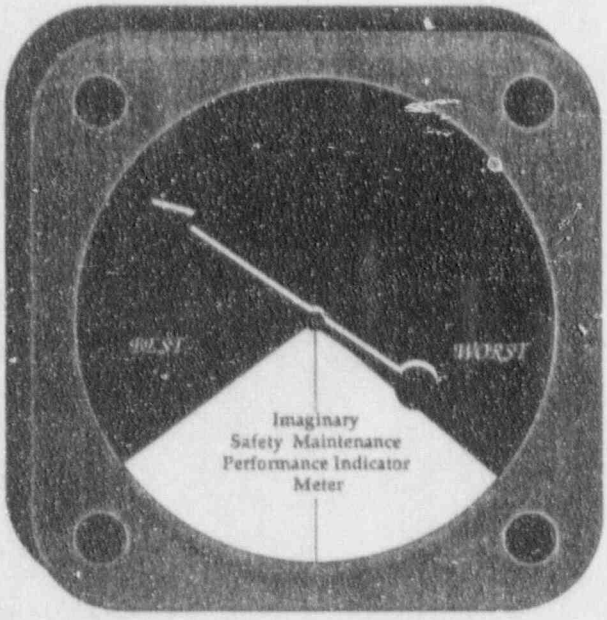
TRENDING PLANT PERFORMANCE

THOUGHTS ON RISK-BASED PERFORMANCE INDICATORS

JOSEPH R. FRAGOLA
VICE PRESIDENT
SCIENCE APPLICATIONS INTERNATIONAL CORPORATION
8 WEST 40TH STREET
14TH FLOOR
NEW YORK, NEW YORK 10018

AEOD WORKSHOP
ANNAPOLIS, MARYLAND
JANUARY 29 & 30, 1992

THE ELUSIVE PERFORMANCE INDICATOR METER



PERFORMANCE INDICATOR CONCEPTS

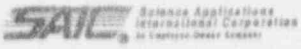
U.S. NRC performing R&D on performance indictors since 1986

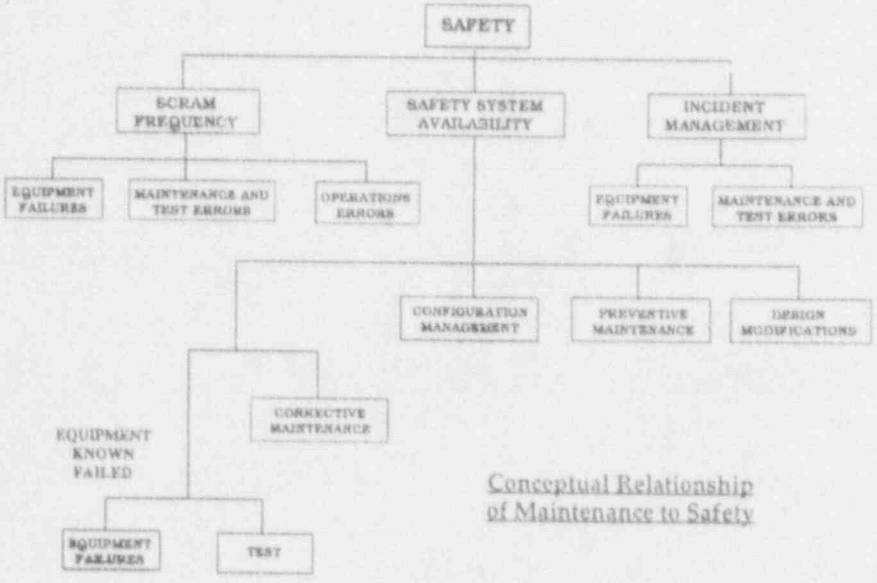
The term "Performance Indicator" reflects a set of data that should have correlation with individual plant safety performance (SECY – 86 – 317)

Performance Indicators are ONE part of a *Performance Management System*

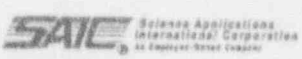
Two types of Performance Indicators:

- Direct
- Programmatic





Conceptual Relationship of Maintenance to Safety

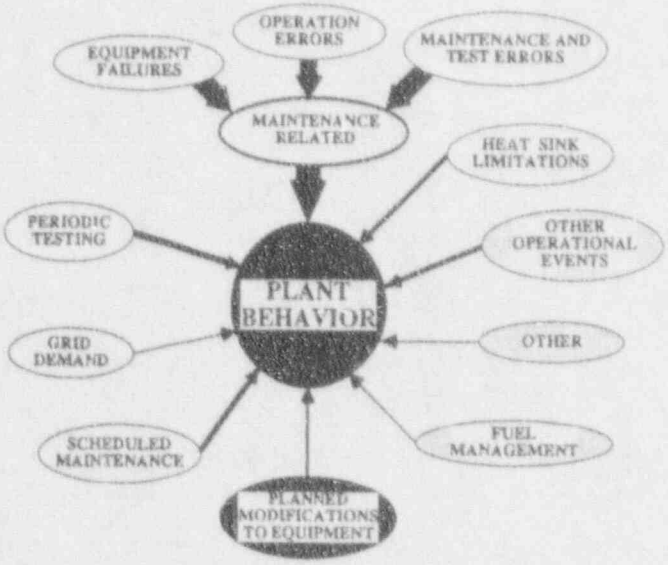


RATIONALE FOR THERMAL EFFICIENCY AS AN INDICATOR

- Safety and Thermal Efficiency both depend on high quality plant maintenance
- The non-safety-related portion of the plant continuously generates information during operation
- While the safety-related-portion depends on either passive features or standby systems whose status is only known intermittently
- Long term neglect of maintenance needed for the plant to fulfill its basic mission - *generating electrical energy efficiently* - may indicate an even greater neglect of the nuclear safety functions
- Reactor scrams and safety system challenges are mainly attributable to BOP system and component failures

SAIC Science Applications International Corporation

Causes of Parameter Fluctuations



Note: arrow and line size denote relative contribution to fluctuations on plant behavior

SAIC Science Applications International Corporation

Average Daily Power level As An Indicator Source

The driving factors are based on the initial requirements set forth by the Commission in SECY - 86 - 317

- **Broad Based** : The indicator should sense effects from maintenance, operations, engineering, management, etc.
- The indicator must be related to safety
- No new data, or reporting requirements
- The indicator should not be focused on comparing plants
- The indicator should be objective

SAIC Science Applications International Corporation

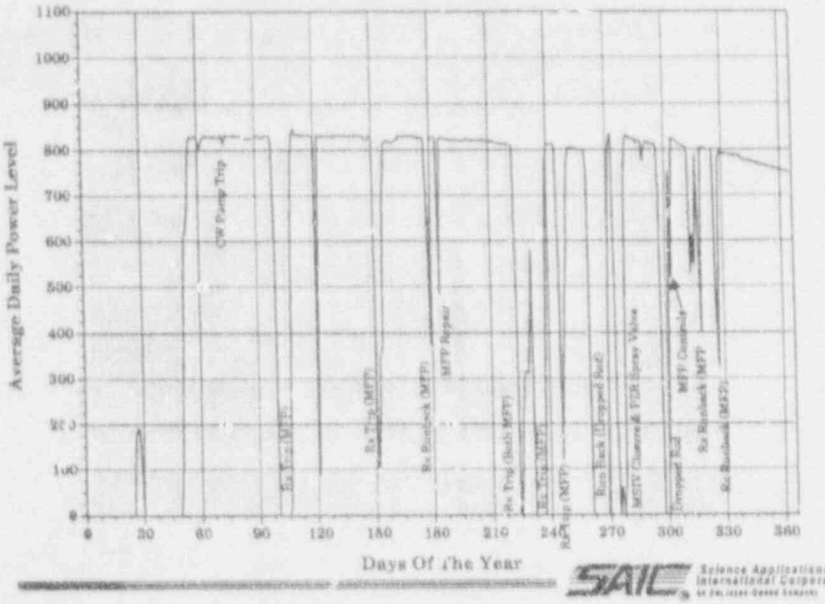
INITIAL ANALYSIS

- Fast Fourier Transforms and Power Spectrum Densities
- Standard Heat Rate Analysis
- Other Mathematical Transformations

SAIC Science Applications International Corporation

PLANT "X" 1985

ANNOTATED WITH EVENTS



SAIC Science Applications International Corporation

Characterizations Of Average Daily Power Level

The general plant behavior can be typically characterized by:

- Average Power Level
- Time Rate of Change of the Power Level
- Number and Magnitude of the Power Losses (Fluctuations)

SAIC Science Applications International Corporation

CHARACTERIZATIONS OF THE OUTPUT BEHAVIOR OF A PLANT

FROM THE ANALYSIS OF AVERAGE DAILY POWER LEVEL DATA

1. High Instability - Characterized by many power losses

2. High Instability at Low Power Levels - Characterized by many power losses at a low power level

3. High Instability After a Long Outage - Characterized by many power losses or several scrams occurring right after a lengthy outage (≥ 1 month)

4. Continous Low Power Operation - Operation at lower than 60% average power

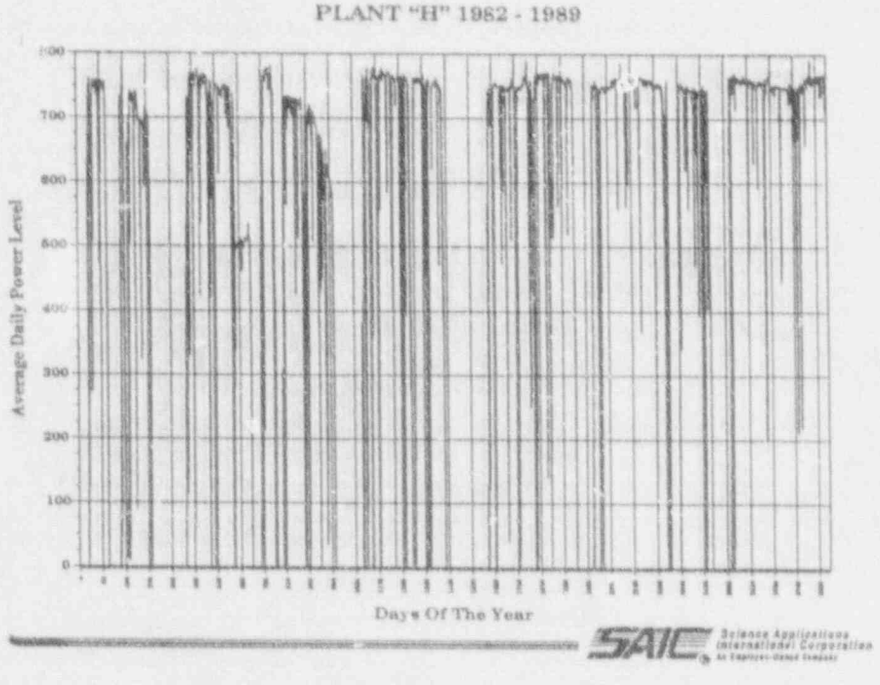
5. Operation at Decreasing Power Levels - Power level decreasing for no apparent reason

6. Operation at a Decreasing Power Level Combined with a High Instability

7. Scrams Occurring at a Low Power Level

8. A Large Number of Scrams (large power loss) at Any Power Level

SAIC Science Applications International Corporation



SAIC Science Applications International Corporation

MEASUREMENT OF PARAMETERS

- **Average Power Level**
  Normalized Percent Average Power Level, based on Net Maximum Dependable Capacity

- **Time Rate of Change of the Power Level**
  The Direction of the Slope of the Change in Power Level Per Time (magnitude is ignored)

- **Number and Magnitude of the Power Losses (Fluctuations)**
  The Number and Magnitude of the Power Losses, for a given time period

SAIC Science Applications International Corporation

PLANT OUTPUT BEHAVIOR CHARACTERIZATION "RULES OF THUMB"

1. **POWER LEVEL**
   - HIGH (H), ≥ 80%
   - MODERATE (M), ≥ 60% and < 80%
   - LOW (L), ≥ 40% and < 60%
   - VERY LOW (V), < 40%

2. **POWER RATE**
   - INCREASING (I)
   - CONSTANT (C)
   - DECREASING (D)

3. **POWER LEVEL INSTABILITY**
   - *(f) = fluctuation 1*, 0% - 5% average power loss and ≥ 15 losses but < 25 losses
   - *(F) = Fluctuation 2*, 0% - 5% average power loss and ≥ 25 losses
   - *(L) = Low Instability*, 5% - 25% average power loss and ≥ 10 losses
   - *(H) = High Instability*, 25% - 50% average power loss and ≥ 5 losses
   - *(S) = Significant Instability*, 50% - 100% average power loss and ≥ 3 losses

NOTE: If power level = V (≤ 40%), a determination of outage and other investigation is required.

These characterizations are combined to produce an ***OUTPUT BEHAVIOR MATRIX***, where the first character identifies the Power Level, the second character identifies the Power Rate, and the third through sixth characters identify the Instability.

SAIC Science Applications International Corporation

Combination of Parameters

These individual characterizations are then combined to produce all possible combinations of the plant output behavior

---

The com`inations were then placed in a non - mathematical matrix to allow for bining of different plant output behavior groups

---

The 5 different groups differentiate high quality from poor quality maintenance, as defined in the broad sense here

NRC FORM 335 (2-89) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER (Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)

NUREG/CP-0124

2. TITLE AND SUBTITLE

Workshop on the Use of PRA Methodology for the Analysis of Reactor Events and Operational Data

3. DATE REPORT PUBLISHED

MONTH: June | YEAR: 1992

4. FIN OR GRANT NUMBER

5. AUTHOR(S)

D.M. Rasmuson, U.S. Nuclear Regulatory Commission
S. Dingman, Sandia National Laboratories

6. TYPE OF REPORT

Final

7. PERIOD COVERED (Inclusive Dates)

January 29-30, 1992

8. PERFORMING ORGANIZATION – NAME AND ADDRESS (If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)

Division of Safety Programs
Office for Analysis and Evaluation of Operational Data
U.S. Nuclear Regulatory Commission
Washington, DC 20555

9. SPONSORING ORGANIZATION – NAME AND ADDRESS (If NRC, type "Same as above"; if contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)

10. SUPPLEMENTARY NOTES

11. ABSTRACT (200 words or less)

A workshop entitled"The Use of PRA Methodology for the Analysis of Reactor Events and Operational Data" was held on January 29-30, 1992 in Annapolis, Maryland. Over 50 participants from the NRC, its contractors, and others participated in the meetings. During the first day, presentations were made by invited speakers to discuss issues in relevant topics. On the second day, discussion groups were held to focus on three areas: (1) risk significance of operational events, (2) industry risk profile and generic concerns, and (3) risk monitoring and risk-based performance indicators. Summaries of the discussion sessions are contained in the report as well as important insights gained from the discussions.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)

Probabilistic Risk Analysis
Performance Indicators
Accident Sequence Precursors
Event Analysis

13. AVAILABILITY STATEMENT

Unlimited

14. SECURITY CLASSIFICATION

(This Page)
Unclassified

(This Report)
Unclassified

15. NUMBER OF PAGES

16. PRICE

THIS DOCUMENT WAS PRINTED USING RECYCLED PAPER

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001