SAFETY AND RELIABILITY DIRECTORATE

PROCEEDINGS OF THE CSNI WORKSHOP

ON

PROBABILISTIC SAFETY ASSESSMENT

AS AN AID TO

NUCLEAR POWER PLANT MANAGEMENT

BRIGHTON
MAY 1986

Hosted by the UKAEA/SRD

Editor : N J Holloway

UNITED KINGDOM ATOMIC ENERGY AUTHORITY
Wigshaw Lane, Culcheth Warrington
WA3 4NE
Proceedings of the CSNI Workshop on Probabilistic Safety Assessment as an Aid to Nuclear Power Plant Management
Brighton, UK May 1986
edited by N J Holloway

FOREWORD

This workshop was organised by the Safety and Reliability Directorate of the United Kingdom Atomic Energy Authority on behalf of Principal Working Group 5 of the Committee on the Safety of Nuclear Installations.

The intention of Principal Working Group 5 (Risk Assessment) was that this workshop would act as the starting point for a Working Group Task with the same title, leading to production of a report in late 1987. Task Force 7 of Principal Working Group 5 has been set up to perform this task.

S.R.D.
November 1986
CONTENTS

Workshop Programme

List of Papers (in order of presentation)

List of Papers (by subject area)

Salient Points from the Questions and Discussions on the
Presented Papers

Discussion A (Utilities)

Discussion B (Regulators)

Plenary Discussions and Participants' Recommendations to
the CSNI Task Force

Chairman's Summary of the Workshop

List of Participants

Workshop Papers
WORKSHOP PROGRAMME

ORGANISATION FOR ECONOMIC
CO-OPERATION AND DEVELOPMENT

NUCLEAR ENERGY AGENCY

SINDOC (86) 69

STEERING COMMITTEE FOR NUCLEAR ENERGY

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

PRINCIPAL WORKING GROUP No.5 - RISK ASSESSMENT

FINAL PROGRAMME FOR A WORKSHOP

entitled

PROBABILISTIC SAFETY ASSESSMENT

AS AN AID TO

NUCLEAR POWER PLANT MANAGEMENT

MAY 20-23 1986

Brighton, UK

UK Organisers: Safety & Reliability Directorate
UK Atomic Energy Authority
Wigshaw Lane
Culcheth
Warrington WA3 4NE, UK

CSNI Organisers: Task Force 7, Principal Working Group 5

N J Holloway (SRD) United Kingdom (Chairman, TF 7)
P M Herttrich(BMI) West Germany ( " , PWG 5)
H P Balfanz (TuV) " "
P Gumley (AECL) Canada
R Virolainen(STUK) Finland
J Caisley (NEA) Paris (Secretary, PWG 5)

Sponsored by Electrowatt UK

Visit to Dungeness 'B' by courtesy of CEGB South East Region
INDICATIVE TECHNICAL TOPICS

THE FOLLOWING TECHNICAL TOPICS ARE LISTED AS INDICATORS OF THE TECHNICAL SCOPE OF THE WORKSHOP

Objectives of reliability analysis and assurance in the management of Nuclear Power Plant safety.

Interfacing between reliability or risk assessment methods and plant management.

Systems for indicating the safety status of plant during operations and maintenance.

Ranking methods for identifying risk-important elements and systems

Quick look techniques for rapid decisions (e.g. startup/shutdown)

Use of PSA techniques in reliability/availability improvement, including maintenance scheduling etc.

Specific applications of PSA to NPP management decisions.

Experience with reliability data collection on NPPs.

Use of reliability analysis in setting technical specifications.

Relating reliability targets to risk targets - selection of the basis for operational or design targets.

Regulator's experience with PSA as a decision tool.

Comparisons of PSA with alternative decision tools for NPP management.

Use of PSA in training plant operators or management personnel.

Construction of 'living PSA models' of operating plants.

Possible conflicts of PSA based decisions with other decision bases.

GUIDANCE TO PARTICIPANTS

WORKSHOP LANGUAGE: ENGLISH

There is no pre-set format for papers, nor any requirement to provide copies in advance of the meeting. However, a title and short (up to 100 word) abstract, received by the end of April, will be appreciated.

Authors are requested to bring 40 copies of papers for distribution at the workshop, or, where papers are not to be circulated, 40 copies of an abstract or other 'aide memoire' for the papers.

Speculative presentations, not written in the form of papers, will be accepted in the workshop, particularly in sessions 4, 5, and discussions A and B.

SRD will produce a limited number of workshop proceedings, including papers up to 20 pages in length. Publication of papers in these proceedings is subject to individual authors' approval.

Authors/presenters will be advised of the session in which their papers will be taken, within a few days of receipt of title/abstract details.
PROVISIONAL PROGRAMME - SESSION TITLES

SESSION 1
KEYNOTE LECTURES
Three invited lecturers, representing a utility (CEGB), a research organization (SRD), and a regulator (BNI, Germany).

SESSION 2
CURRENT REQUIREMENTS AND METHODS
Papers dealing with requirements already identified in some detail and with methods already implemented, or well advanced towards implementation.

SESSION 3
RELIABILITY ANALYSIS, DATA COLLECTION AND FEEDBACK
Papers dealing with applicable methods of reliability analysis and data collection, with emphasis on existing schemes or those immediately in prospect. Possibilities for feedback between operations and data collection/analysis.

SESSION 4
MODELLING, COST-BENEFIT, EVALUATION
Models which can form the basis for planning and evaluating schemes of PSA support to NPP's. Methods of cost-benefit analysis or other methods of evaluating the impact of PSA schemes on operations. (Emphasis on future planning and methods)

SESSION 5
REGULATORY POSITIONS, UNCERTAINTY, PHILOSOPHY

SESSION 6
SUMMARY, FUTURE PROSPECTS
Review of workshop (by PWG 5 task force representatives)
Discussions of future prospects in the overall subject area.

(Formal papers are not expected for Session 6)

SPECIAL DISCUSSIONS

DISCUSSION A
THE UTILITIES' VIEWPOINT
An informal discussion centred upon the requirements of utilities in the area of NPP management.

DISCUSSION B
THE REGULATORS' VIEWPOINT
An informal discussion on the limits of application of probabilistic methods in plant management, and related aspects of licensing.

Formal papers are not expected for the discussion sessions.
PROGRAMME

TUESDAY, MAY 20
10.00 Opening of Workshop
10.30 SESSION 1
12.30 Lunch
14.00 SESSION 2
18.00 Reception by Electrowatt UK
Evening free

WEDNESDAY, MAY 21
09.00 SESSION 3
11.45 Visit to Dungeness 'B' Advanced Gas Cooled Reactor
13.30 Lunch at Battle (Site of the Battle of Hastings)
19.30 Return to Hotel
20.30 Conference Dinner

THURSDAY, MAY 22
09.00 SESSION 4
12.30 Lunch
14.00 to SESSION 5
17.30
20.30 DISCUSSIONS A and B (in parallel)
(followed by Plenary Discussion)

FRIDAY, MAY 23
09.00 SESSION 6
12.00 Workshop ends
pm Meetings of CSNI PWG 5 task group 7 and other
task groups

DOMESTIC INFORMATION

Brighton is located within 1 hour's journey (train) of Gatwick Airport, and
within 2 hours (Metro/train) of Heathrow Airport.

The Imperial Hotel, venue for the workshop, is just off the Brighton seafront.

Inclusive costs of accommodation and meals at the hotel are approximately £42 per
day, based on single room occupancy. Costs of non-residential attendance,
including lunch, coffee, tea, etc, are approximately £12.50 per day.

Participants are requested to advise the workshop chairman or secretary of their
travel arrangements and accommodation requirements.

Chairman
N J Holloway

Secretary
Ruth Campbell

SRD, Wigshaw lane
Culcheth
Warrington WA3 4NE
United Kingdom
Tx 629301 ATOMRY G

Ext 7316
Tel 0925-31244
Ext 7243
CSNI WORKSHOP ON

PROBABILISTIC SAFETY ASSESSMENT
AS AN AID TO NUCLEAR POWER PLANT MANAGEMENT

20-23 May 1986

Brighton, UK

LIST OF PAPERS

SESSION 1  (Chairman: P M Herttrich)

1. P A Corkerton  Utility perspective on PSA as an aid to NPP management.

2. N J Holloway  Can PRA Pay?

3. P M Herttrich  Regulators perspective on PSA as an aid to NPP management.

SESSION 2  (Chairman: G M Ballard)

   A Piirto
   J Vanhala
   T Mankamo
   U Pulkkinen


6. V Cavicchia  Overview of the probabilistic safety studies for nuclear power plants in Italy. Points of view and prospects for the utilization of the probabilistic methodology.
   M Nobile
   S Serra

7. A Valeri  The use of PSA for safety decisions in the Italian PWR programme.
   C Zaffiro

8. V M Raina  Application of probabilistic safety assessment to the safety design verification of Darlington Nuclear Generating Station.

   T Schaubel
   K Serdula

    K Serdula

SESSION 3  (Chairman: M H Lee)

11. B E Horne  The use of PSA techniques in a CEGB power station operational environment.
<table>
<thead>
<tr>
<th></th>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>H Hoertner&lt;br&gt;W Frey&lt;br&gt;J von Linden&lt;br&gt;G Reichart</td>
<td>German precursor study – methods and results.</td>
</tr>
<tr>
<td>13</td>
<td>P Homke&lt;br&gt;E Lindauer&lt;br&gt;C Verstegen</td>
<td>Influences on the failure behaviour of components and their importance for the credibility of PSA-results.</td>
</tr>
<tr>
<td>14</td>
<td>J K Vaurio</td>
<td>Objectives and methods of reliability data collection and analysis at Lovisa Power Plant.</td>
</tr>
<tr>
<td>15</td>
<td>H W Kalfsbeek</td>
<td>Merging reliability modelling and operating experience assessment.</td>
</tr>
<tr>
<td>16</td>
<td>P Humphreys</td>
<td>Dependent failures data collection.</td>
</tr>
<tr>
<td>17</td>
<td>M V Bonaco</td>
<td>The role of probabilistic risk assessment in support of nuclear plant operation and safety, a northeast utilities perspective.</td>
</tr>
<tr>
<td></td>
<td><strong>SESSION 4</strong> (Chairman: H Witt)</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>S Sahgal&lt;br&gt;A Torri</td>
<td>Risk-benefit evaluation of backfit options at nuclear power plant Beznau.</td>
</tr>
<tr>
<td>19</td>
<td>H Campbell</td>
<td>Use of PSA for research reactor management.</td>
</tr>
<tr>
<td>20</td>
<td>P Humphreys&lt;br&gt;B D Johnston</td>
<td>Problems arising in PSA based management due to dependent failures.</td>
</tr>
<tr>
<td></td>
<td><strong>SESSION 5</strong> (Chairman: S Chakraborty)</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>N J Holloway</td>
<td>Which risk-related quantities should be managed?</td>
</tr>
<tr>
<td>22</td>
<td>T P Speis&lt;br&gt;A A El-Bassioni</td>
<td>PSA regulatory applications at USNRC.</td>
</tr>
<tr>
<td>23</td>
<td>J C Glynn</td>
<td>A PRA based interactive system for planning reactor inspection activities (presented by Dr J Jenkins).</td>
</tr>
<tr>
<td>24</td>
<td>A R Diederich</td>
<td>Use of the Limerick PRA in safety assurance.</td>
</tr>
<tr>
<td>25</td>
<td>A R Garlick</td>
<td>The requirements of uncertainty analysis.</td>
</tr>
<tr>
<td>26</td>
<td>M H Lee</td>
<td>The use of predictions of uncertainty in PSA.</td>
</tr>
</tbody>
</table>
LIST OF PAPERS BY SUBJECT AREA

(Papers may appear under several headings)

Paper numbers refer to the order of presentation list.

Applications to Current Plants
4, 6, 9, 17, 18, 19, 24.

Applications to Plants under Design
1, 6, 7, 8, 24.

Future Prospects
1, 2, 3, 6, 21.

Applications to Maintenance/Technical Specifications
4, 10, 11, 17, 24.

Applications to Backfitting
9, 17, 18, 19.

Applications to Regulation
3, 7, 22, 23.

Reliability Data Collection and Analysis
10, 12, 13, 14, 15, 16.

Computer Aids
11, 23.

Quality Assurance
5, 10.

PSA Theory and Decision Theory
2, 20, 21, 25, 26.

Uncertainties
2, 13, 14, 20, 25, 26.
NOTE

This workshop took place within a month of the Chernobyl reactor accident. The presented papers, prepared before the occurrence of the accident, do not therefore take any account of it. However, its occurrence had an influence on the discussions at the workshop and clearly contributed to the idea that PSA should be increasingly applied to nuclear power reactors.
Salient Points from the Questions and Discussions on the Presented Papers

No detailed records of questions and discussions was kept - the following points were noted as salient points made in the discussions. They are not attributed:-

The real goal of any approach to safety must be that no accidents should happen.

It is important to make PSA suitable for practical decisions, not just for estimating risks.

PSA numbers should be used according to the manufacturer's instructions - other uses may be inappropriate. (Don't put heavy loads on weakly supported numbers!)

If probabilistic methods are used to justify a plant, why not use them to operate it?

Experience has shown that early use of PSA can lead to inexpensive but effective modifications.

Modifications motivated by PSA have led to unintentional paybacks in availability.

Major benefits of PSA are in improved perspectives, not bottom line numbers.

PSA can be used to rationalise the deterministic process.

The best method for uncertainty (into the sources and nature of the uncertainty) analysis is the one which gives the best insights.

Transfer of results from one plant to another can be misleading.

"Risk is part of everyone's work".
THE DISCUSSION SESSIONS

Evening discussion sessions were held at the Workshop. Discussion A contained the utility representatives while discussion B contained the regulatory representatives, while research organisation representatives could attend either.

Similar, but slightly different 'motions' were put up to these discussions to initiate the debate. In both cases these were modified, although the basic tenet that level 1 PRA should be performed for all nuclear plants was retained in both discussions.

A brief record of the discussions follows. Statements are not attributed to specific persons or organisations.
DISCUSSION A (UTILITIES)

Chairman : M Bonaco, Northeast Utilities, USA

The discussion session was presented with the following motion:-

"Level 1 PSA should be performed for all nuclear power plants within the next 5 years.

Reasons

Experience of plant-specific PSA has shown that benefits in:

- Increased safety
- Increased availability
- Increased understanding

are more than necessary to repay the PSA costs."

Almost immediately, a high level of consensus emerged that a specific timescale was not desired by the utilities, but that 'as soon as possible' should be substituted for 'in the next 5 years'.

Most participants in the discussion thought that regulators would impose some requirement to perform PSA upon them quite soon, but gave the impression that this would not be particularly unwelcome.

There was a general consensus on the possibility of the following benefits of performing level 1 PSA:

(a) Improved understanding of the plant by the utility, at both engineering and management levels.

(b) Provision of a rational basis for discussion with regulators on the subjects of new requirements and backfits.

These benefits would only accrue to the utilities if they themselves participated strongly in the PSA. Although aid in the performance from consultants was not excluded, the method sometimes practiced in the past, whereby consultants were brought in to manage and perform most of the work, was not thought to be as useful since the utility did not thereby learn from the experience of PSA performance.

There was less consensus on the matter of direct financial payback in availability or savings on maintenance etc. While some plant operators had reported identifiable savings which amounted to more than the PSA costs, others were doubtful about this possibility. In particular, some plants already had high availability, so there was little increase possible, and other plants had unavailability caused by design faults not related to safety. Perhaps it was true to say that the majority of utilities who had actually done the PSAs had achieved payback in one form or another, but that these paybacks were anecdotal rather than predictable. At the moment there are insufficient anecdotes to make a generality.
Since the discussion took place within a few weeks of the Chernobyl accident, the value of PSA in the public domain and as a response to Chernobyl was also discussed. The participants thought that the use of PSA could go either way in the public domain. While risks would be shown to be low, the novelty of PSA results as a way of expressing risks might divert public attention to uncertainty, which would be seen as an undesirable feature, regardless of the assessed risk values. However, some response to Chernobyl would be needed, and PSA based responses remained a possibility.

Thus, in conclusion, the motion put to the discussion survived with the modification that fixed timescales were undesirable. Although the matter of direct financial payback from the performance of PSA was not agreed, the consensus was that the overall payback, including the improved understanding of the plant, would make the exercise worthwhile. However, the utility representatives present acknowledged that they were 'PSA enthusiasts' and might not be representative of utility attitudes overall.
DISCUSSION B (REGULATORS)

Chairman : J Jenkins, USNRC

The following motion was presented to initiate the discussion:-

"(1) Level 1 PSA should be performed for all nuclear power plants within the next 5 years.

(2) Regulatory authorities should provide 2 staff members to work on each station PSA, at the expense of removing them from deterministic safety activities.

Reasons

The PSA activities will prove more beneficial to safety than the 'lost' deterministic activities."

As in the utilities' discussion, the concept of a fixed timescale was not supported, and 'as soon as possible' was substituted. However, the basic tenet that PSA should be performed on all plants was supported.

(Note: In both this and the utilities' discussion, the ability of one PSA to cover for a number of identical plants was recognised, so that the number of assessments would not be equal to the total number of plants.)

The idea that regulators should participate in the PSAs with direct effort was also deleted, although regulatory input to defining the purposes and format of PSA was thought advisable. In general it was a matter for the licensees to prepare and to present their safety case. Regulatory input could follow the normal safety case assessment procedures.

The discussion resulted in a number of suggestions on the way forward, as listed below: (based on the Chairman's notes)

1. PSA should be performed by utilities (rather than by consultants or regulators), and where it is a part of the safety case, used by regulators in assessing safety.

2. Manufacturers of turnkey plants should provide a PSA as part of the delivered product.

3. The purposes of PSA performance need to be further defined.

4. The character, assumptions and limitations of PSA should be made clear to management.

5. Prior experience of operating plants must be used in the validation of PSAs.

6. A standard method of reporting PSA data and results should be developed.
Several recommendations were made by the regulators' discussion group with regard to the role of CSNI/PWG5 in promoting the use of PSA by utilities. These are mentioned in the following record of the plenary discussion.

In general terms, the regulators' group wished to see increasing use of PSA in analysis of plant safety, recognising it as a useful insight which traditional methods had not provided. However, they wished to sidestep the direct question of whether or not the effort in PSA should be at the expense of effort in traditional methods.
PLENARY DISCUSSIONS AND PARTICIPANTS' RECOMMENDATIONS
TO THE CSNI TASK FORCE

(Based on the plenary discussion following the utilities/regulators
sessions and the final discussion session of the workshop)

The plenary discussion sessions provided an opportunity for the workshop
participants to suggest to the CSNI task force some objectives for their
prospective work on the topic of 'PSA as an aid to NPP management', which
is intended to be performed over the next 1 - 1½ years.

The recommended objectives are in no sense mandatory, but have been taken
into account by the CSNI Task Force as subsequent discussions.

Recommendations/Suggestions

1. The actual benefits which utilities have gained from PSA should be
discovered and explained.

2. Specifications of the type of assessment most useful to plant
managers should be developed.

3. The need to 'sell' the ideas to utilities should be addressed.

4. A clear statement of 'what PSA is' should be prepared.

5. The matter of the appropriate level (core melt, release, offsite
consequences - levels 1, 2, 3) should be addressed (there was
considerable discussion on this topic at the workshop, and a clear
lack of general consensus).

6. Questionnaires to utilities to discover what is being done may be
useful.

7. Recommendations should be made on the appropriate data collection
to be undertaken in support/validation of PSA.

8. Guidance should be given on the interpretation of PSA results.

9. The limitations on PSA usefulness, and how these might be
overcome, should be addressed.

10. Emphasis should be placed on the structural aspects of PSA, not on
the achievement of bottom line results.
CHAIRMAN'S SUMMARY OF THE WORKSHOP

Although this workshop, in common with any meeting of this type, exhibited a clear bias towards supporters of PSA rather than its opponents, it was in other ways fairly representative of the various organisations with interests in its chosen subject. In particular, the balance between utilities and regulators was almost ideal, and the balance of representation between OECD countries lacked only France and Sweden amongst the major users of nuclear power.

If one can summarise the theme of the workshop in a single idea, I would do so in the statement, applied to the PSA process, that:

"The journey is more important than the destination"

that is: the structure and information contained within PSA is more important (for the use being considered) than the 'bottom line' risk results. Indeed, in the workshop presentations, very little mention was made of final results, or comparisons with risk criteria, while much was made of the identification of accident sequences, prioritization of issues, education of operators, effects on availability and maintenance, etc; all of which derived from the 'middle lines' of the process rather than from the 'bottom lines'.

The papers, particularly those from the utilities which expounded practical experiences and imminent uses, provided ample indications of how the task should be progressed, as did the many suggestions made by the workshop participants. It is hoped that the CSNI Task Force will (in its forthcoming task) be able to fulfil some of the expectations of the participating organisations and to promote the exploitation of PSA for the benefit of nuclear safety and power production.
## List of Participants

**OECD**
- J Caisley: Nuclear Safety Division, Nuclear Energy Agency

**Australia**
- H Witt: Australian Atomic Energy Commission

**Canada**
- R Comeau: Gentilly 2 Nuclear Generating Station, Hydro Quebec
- V Raina: Design & Development /Generation, Ontario Hydro

**Finland**
- A Piirto: Teollisuuden Voima Oy Industrial Power Company Ltd
- J Vaurio: Imatran Voima Company
- R Virolainen: Finnish Centre for Radiation & Nuclear Safety

**West Germany**
- H Balfanz: Technischer Überwachungs-Verein Norddeutschland eV
- P Herttrich: Division of Reactor Safety, Federal Ministry of the Interior
- H Hoertner: Gesellschaft für Reaktorsicherheit (GRS) mbH
- P Homke: Gesellschaft für Reaktorsicherheit (GRS) mbH
- J Weber: Kernkraftwerk Krümmel

**Italy**
- V Cavicchia: Ente Nazionale Per l'Energia Elettrica (ENEL)
- H Kalfsbeek: CEC Joint Research Centre
- S Serra: Ente Nazionale Per l'Energia Elettrica (ENEL)
- A Valeri: Ente Nazionale Energie Alternative (ENEA)
- C Zaffiro: Ente Nazionale Energie Alternative (ENEA)

**Japan**
- A Otsubo: Institute of Nuclear Safety
- T Tobioka: Atomic Energy Research Institute

**Spain**
- J Calvo: Consejo de Seguridad Nuclear (CSN)
- R Fernandez: Nuclenor
Switzerland
S Chakraborty Swiss Federal Nuclear Safety Inspectorate
H Hirschmann Swiss Federal Institute for Reactor Research
S Sahgal Nordostschweizerische Kraftwerk AG

United States of America
M Bonaca Reactor Engineering, Northeast Utilities
A Diederich Philadelphia Electric
J Jenkins United States Nuclear Regulatory Commission
T Speis United States Nuclear Regulatory Commission

United Kingdom
M Barents Electrowatt Engineering Services (UK) Ltd
H Campbell Safety and Reliability Directorate
P Corkerton Central Electricity Generating Board
A Danielson South of Scotland Electricity Board
A Debenham Safety and Reliability Directorate
R Dumolo Electrowatt Engineering Services (UK) Ltd
A Garlick Safety and Reliability Directorate
E Gilby Consultant to Electrowatt Engineering Services (UK) Ltd
D Hamblen Central Electricity Generating Board
R Haward Safety & Reliability Directorate
N Holloway Safety & Reliability Directorate
B Horne Central Electricity Generating Board
P Humphreys Safety & Reliability Directorate
M Lee Central Electricity Generating Board
A McArthur Central Electricity Generating Board
I Matcher Central Electricity Generating Board
J Rixon Nuclear Installations Inspectorate
S Ryan Central Electricity Generating Board
R Sale Central Electricity Generating Board
J Smith Safety and Reliability Directorate
G Waplington Electrowatt Engineering Services (UK) Ltd
WORKSHOP PAPERS
CSNI WORKSHOP ON

PROBABILISTIC SAFETY ASSESSMENT
AS AN AID TO NUCLEAR POWER PLANT MANAGEMENT

10–23 May 1986
Brighton, UK

LIST OF PAPERS

SESSION 1  (Chairman: P M Herttrich)

1. P A Corkerton  Utility perspective on PSA as an aid to NPP management.

2. N J Holloway  Can PRA Pay?

3. P M Herttrich  Regulators perspective on PSA as an aid to NPP management.

SESSION 2  (Chairman: G M Ballard)

4. M Kosonen
   A Piirto
   J Vanhala
   T Mankamo
   U Pulkkinen  Experiences of the use of PSA methods at the TVO Power Plant.


6. V Cavicchia
   M Nobile
   S Serra  Overview of the probabilistic safety studies for nuclear power plants in Italy. Points of view and prospects for the utilization of the probabilistic methodology.

7. A Valeri
   C Zaffiro  The use of PSA for safety decisions in the Italian PWR programme.

8. V M Raina  Application of probabilistic safety assessment to the safety design verification of Darlington Nuclear Generating Station.

9. R Comeau
   T Schaubel
   K Serdula  Revision of Gentilly 2 Safety Design Matrix Studies.


SESSION 3  (Chairman: M H Lee)

11. B E Horne  The use of PSA techniques in a CEGB power station operational environment.
12. H Hoertner  
    W Frey  
    J von Linden  
    G Reichart  
    German precursor study – methods and results.
13. P Homke  
    E Lindauer  
    C Verstegen  
    Influences on the failure behaviour of components and their importance for the credibility of PSA-results.
14. J K Vaurio  
    Objectives and methods of reliability data collection and analysis at Lovisa Power Plant.
15. H W Kalfsbeek  
    Merging reliability modelling and operating experience assessment.
16. P Humphreys  
    Dependent failures data collection.
17. M V Bonaco  
    The role of probabilistic risk assessment in support of nuclear plant operation and safety, a northeast utilities perspective.

SESSION 4  (Chairman: H Witt)
18. S Sahgal  
    A Torri  
    Risk-benefit evaluation of backfit options at nuclear power plant Beznau.
19. H Campbell  
    Use of PSA for research reactor management.
20. P Humphreys  
    B D Johnston  
    Problems arising in PSA based management due to dependent failures.

SESSION 5  (Chairman: S Chakraborty)
21. N J Holloway  
    Which risk-related quantities should be managed?
22. T P Speis  
    A A El-Bassioni  
    PSA regulatory applications at USNRC.
23. J C Glynn  
    A PRA based interactive system for planning reactor inspection activities (presented by Dr J Jenkins).
24. A R Diederich  
    Use of the Limerick PRA in safety assurance.
25. A R Garlick  
    The requirements of uncertainty analysis.
26. M H Lee  
    The use of predictions of uncertainty in PSA.
A Utility Perspective on

Probabilistic Safety Assessment as an Aid to

Nuclear Power Plant Management

P A Corkerton

Health & Safety Department
Central Electricity Generating Board, London

1. Introduction

Probabilistic safety assessment methods have now been under development and in use in various forms in the nuclear industry in the United Kingdom for over twenty years. Progress in the development of analysis techniques and general acceptance of this technology has been slow because for a long time people in the nuclear industry in general, and particularly those who influenced or set safety standards, were afraid of this new and different approach to the assessment of acceptable safety standards. Therefore various reasons were given why the technology was fundamentally acceptable but was never quite ready for use.

However, the position has now been reached where most countries with a nuclear industry accept that probabilistic safety assessment is a very useful, and some may say an essential, input into the decision as to whether a nuclear power station is acceptably safe or not. Indeed, there is now considerable international agreement on the need to carry out probabilistic assessments, the use to which such assessments can be put and the measures of acceptability for a PRA. There is also a common understanding of the shortcomings and uncertainties of this technology and therefore the care which is needed in undertaking this type of analysis and the need to ensure that it is in the correct context in the decision making process.

2. Present Uses of PRA

The present uses of PRA cover the design and assessment of the reliability of reactor safety systems, the assessment of the probability of defined core states such as the probability of core melt, the setting of actual hazard criteria by studying the probability of occurrence of such hazards as earthquakes, the assessment of the probability of accidental releases of radioactivity to the atmosphere or doses or risks to members of the public. There are however aspects of the analysis which could be improved and refined. These are the adequacy of available data, the accuracy of the mathematical modelling of nuclear systems and plant, the treatment of common cause effects, the completeness of the analysis, the accuracy of the final number and the validation of the result. There are therefore areas where further work needs to be done to improve our understanding and to develop better mathematical tools for those aspects of PRA with which currently there are difficulties. However PRA, even in its present imperfect statement of development, gives insights into the way systems perform and interact which are not available by any other available technique. It is an extremely powerful assessment tool in the determination of the adequacy of a reactor safety system or of the overall safety of a nuclear power plant in that it ensures designers and safety assessors work within a disciplined, systematic framework which is a necessary pre-requisite for attaining the
high level of safety which the nuclear industry aspires or indeed any other field of industrial activity.

3. Future Uses of PRA

In addition to the present uses of PRA, which will undoubtedly be improved and developed for some time to come, there are many other areas where its use will aid and refine expert judgement in the future. Its use for judging priorities in the research and development field will be expanded as will its use in helping to decide where best to devote resources, both money and technical expertise, to the improvement of safety for the future. It will also be used to improve operating and maintenance strategies on nuclear power plants, assist in the development of improved aids for nuclear operations staff and permit the use of expert systems. It will be used to judge the effectiveness of deterministic safety criteria, which will always form an essential part of nuclear safety criteria and standards, and the merits of proposed changes to such criteria and standards. Such uses are already being discussed in many countries and steps are now being taken to bring some of these to fruition. Other uses such as an aid to emergency planning and accident management whilst not yet even being discussed could all benefit from the rigorous and systematic application of PRA techniques.

The long term aim must be to develop PRA to the state where it is generally accepted by industry, regulators, legislators and by the general public. To do this it is necessary to demonstrate that it can provide an objective assessment of the risk to public health and safety from any industrial activity. If this can be achieved then it would go a long way to making some of the necessary but unpopular industrial decisions at least understandable to the public. Also it would make such decisions at least more logical and less dependent on individual expert judgements which are at present a mixture of an individual's previous experience, personal prejudices and present allegiances.
Foreword

The use of probabilistic risk assessment (PRA) for the estimation of risks in nuclear power plant operations is becoming well established, with examples of its use in many different countries.

The performance of PRA is initially an expense to be incurred within the nuclear industry, and it of some interest to inquire whether or not that expense can result in a worthwhile payback, in increased safety, reduced costs, or other results of better informed management of risks in nuclear operations.

Contents

1. INTRODUCTION
1.1 Perspectives on Risk Management

2. THE QUANTIFICATION OF ACTUAL RISKS
2.1 PRA Procedures - Actual and Nominal Assessment
2.1.1 Prospects for more realistic risk assessment
2.1.2 Prospects for rule based assessments

3. THE SCOPE FOR RISK MANAGEMENT IMPACT ON COSTS
3.1 Actuarial costs of accidents
3.2 Costs of safety design and operation
3.3 Plant unavailability costs
3.4 Conclusions from cost impact discussions

4. POSSIBILITIES FOR PRA BASED RISK MANAGEMENT
4.1 Risk management for plant outage situations
4.2 Risk management for design of systems and operations
4.3 Risk management for reduction of accident frequencies
4.4 Summary of possibilities

5. ANTICIPATED PROBLEMS ARISING FROM PRA UNCERTAINTIES
5.1 Systems analysis uncertainties
5.2 Phenomenological uncertainties
5.3 Discussion

6. CONCLUSIONS
ABSTRACT

This paper discusses the possible uses of Probabilistic Risk Assessment (PRA) concepts in improving the cost-effectiveness of safety management in nuclear power plant design and operations.

The ability of PRA to assess risks realistically is an important aspect of effective management. Because of certain traditional approaches to assessments, realistic results are not always achieved, particularly where pre-set assessment rules are used instead of approximations to realism. The prospects for achieving the realism of assessment necessary for effective risk management are thought to be good, provided that rule based methods are largely avoided. Realistic assessments are likely to involve large uncertainties, and the management of risks in the presence of these uncertainties is discussed.

The cost-effectiveness of PRA based risk management is likely to be achieved most easily in those areas of nuclear operations where the cost differences between alternatives is greatest. The area of greatest potential effectiveness appears to be that of plant availability, as influenced by safety considerations. A single day of avoided outage, resulting from more efficient achievement of safety, repays the same order of costs as a PRA for management purposes is likely to incur.

Risk management in system safety design is also potentially cost-effective, although the possible gains are somewhat lower than in availability management. The area of least potential effectiveness is in risk reduction itself, since the risks from nuclear power plants already have very low actuarial equivalent values. This may be somewhat surprising since this area is the traditional area for the use of PRA methods.

The conclusion of the discussion is that the most promising area for the application of PRA methods is in the management of the safety/availability interface of a nuclear power plant, in such matters as will affect startup/shutdown decisions.
INTRODUCTION

Probabilistic risk assessment (PRA) techniques have been developed in the nuclear industry for the purpose of assessing risks which can arise from nuclear plant operations, particularly those of nuclear reactors. Since the minimization of risks is one of the paramount concerns in reactor operation and regulation, it is useful to be able to identify the reasons why risks arise, and to quantify those reasons and the risks associated with them. Correct identification and quantification is clearly valuable in any scheme for managing, constraining, or preventing risks, in fulfilment of the minimization (ALARA) principles which lie at the foundation of nuclear safety philosophy. It is the possibility of risk management which forms the subject of this paper.

1.1 Perspectives on Risk Management

The management of anything is normally carried on in order to achieve some objective. In the management of nuclear risks/safety, the exact objective is not well defined, and contains some elements from the following approaches to risk management, without aligning with any one in its entirety:

1) Specific target achievement
   UK reactor design principles do not contain explicit risk targets, but do contain some specific targets for events which may lead to public harm. These are concerned with the frequencies of exceeding a plant design basis, or specified (ERL) releases of activity from the site. The achievement of, or near approach to, specific intermediate targets is one important aspect of risk management, and features strongly in the current UK approach to reactor design as exemplified by the CEBG design safety guidelines and the NII design principles.

2) Technical achievability
   The ALARA principle does not explicitly state the concept of achievability involved, and for most of the history of reactor safety, the technical achievability of safety has been the driving force, so that system reliabilities or qualities at the limit of current capabilities have been demanded for the key systems and components in nuclear reactors. However, the use of technical achievability alone leads inexorably to more stringent requirements and higher costs, so that there is now an increasing tendency to moderate this approach with cost considerations, as discussed next:

3) Cost-effectiveness
   The reduction of risks normally involves increased use of society's resources, for which there are substantial competing demands, and at some level these competing demands will exceed the demands for reduction of risks. There are two aspects to the inclusion of costs in the concept of 'reasonably achievable'
   a) The effective use of costs in the management of risk within an overall cost constraint.
   b) The setting of the overall constraint.

The former is the process of optimisation of resources internal to a nuclear safety related project, while the latter extends to a wider optimisation in society. Since the two are almost independent, we shall consider largely the former - the optimisation of existing or fixed resources in the achievement of safety within a project.

Risk management based on PRA can in principle be used to achieve any of the three types of objective. Its success in so doing is dependent upon several factors, including:

a) The availability of quantified risk information
b) The ability to quantify the effects of management actions on risks.
c) The ability to assess costs of management actions (for the cost-related management objectives)
d) The flexibility of the licensing regime to accommodate risk management.

The present paper concentrates on the first two aspects of the above. The cost aspects are not directly addressed, but are presumed to be tractable at the same or a better level of accuracy than the risk assessments. The UK licensing system is one of the more flexible in the world, and there seems no obvious reason why some degree of risk management would not be allowed within it, provided that such management was seen to be in pursuit of the overall principles laid down by the regulators (NII).
2. THE QUANTIFICATION OF ACTUAL RISKS

The management of some quantity becomes a rather meaningless concept unless the quantity itself is amenable to assessment. Since there are various aspects of risks which could be managed, and varying associated degrees of assessment capability, we should be concerned to determine which aspects can sensibly be managed, and to what degree PRA can provide the information to do so.

The development of PRA to date has shown some fairly clear trends in magnitudes and uncertainties of risks, as expressed in the various stages of the procedures, which pass through initiating events, system failures, containment studies, and offsite effects. In general, these are:

- Net contributions to risk increase with accident severity. (i.e. increased severity is not normally offset by reduced frequency - at least up to the point of activity release)
- Uncertainties in assessments increase as accident analysis progresses from systems analysis to offsite effects.

These trends are not conducive to the management of risks, in that they show that the public risks which are normally regarded as the driving factor in nuclear safety are associated with the extremes of accident severity (and therefore unfamiliarity) and the end points of long and cumulative uncertain assessment procedures - quite in the least accessible parts of reactor analysis and experience. Therefore, we do well to ask if there is some point in looking at more accessible parts of the analysis, even though these may reflect something other than the public risks which are envisaged as the underlying concern in nuclear safety. The more accessible, though still quite remote, points of assessment have in the past been centred upon core meltdown accidents. These may not have much direct relationship to public harm in view of the containment possibilities, but they do represent major accidents, and possibly the dominant accidents in terms of overall expected losses on and off the reactor site.

We now look at the possibilities for risk quantification, both at the 'bottom line' public harm levels, and at the intermediate level of core meltdown (or severe core damage).

2.1 PRA Procedures - Actual and Nominal Assessment

A review of historical procedures in PRA reveals that there is little consistency of approach to the question of whether assessments should be based upon realistic (mean or best estimate) or limiting evaluation processes. This mixture of approaches has normally pervaded even individual sequence evaluation as well as overall assessments.

An example of this, taken from the Sizewell B PRA (WCAP 9991) is as follows:

Sizewell B Sequence AE (Large LOCA / loss of component cooling) (sequence to core melt only)

This sequence commences with a nominal large pipe break, which has traditionally been analysed by transient analysis for a guillotine break of a cold leg. The absence of any examples in about 10^7 reactor years of relevant experience formed the primary input to an assessment of frequency of some 10^-7 per year (the precise value used was 0.94 x 10^-3). More detailed assessments of mechanisms of pipe break have led to much lower frequencies, and the expected frequency of the nominal transient is effectively zero as the event specification is at or beyond the limit of physical possibility.

The component cooling system supplies cooling to the emergency injection pumps. Its failure probability was dominated by a common mode assessment limit of 10^-5 failures per demand. This was a design target for the system, because there was little evidence available on the actual common mode failure probability for a system of the proposed type.

The possibility that low head injection pumps would operate for a sufficient time to reflood the core, and that occasional use of the multiply redundant high head pumps could be arranged to continue core cooling was not analysed, as it conflicted with the assumption that operator actions of this type should not be required within the first half hour (too late for this particular defensive try). No specific analysis of operator interference with the defensive systems was incorporated into the analysis of the sequence.

Given the uncertainty inherent in the analysis, it would be rather difficult to view the 10^-5 per year assessed frequency of this sequence in any definitive manner. Clearly the initiating event assessment has the possibility of being very pessimistic, while the CMF assessment may be rather optimistic in relation to past experience, and the repair/operator actions could go either way. Given this type of analysis, which is not atypical, it would be rather difficult
to be definite as to whether this accident deserved consideration in a risk management scheme or not. If to the core melt frequency anal-
ysis we added the source term analysis, which involves containment fail-
ure probabilities and a decidedly pessimistic source term, we would find our views on the relationship of the analysis to reality even more difficult to formulate and justify.

Clearly, we could be in some difficulty by simply reading the results of PRA as the expression of the real risks which we have to try to manage or reduce. The mixture of realistic and nominal assessment which is normally used in PRA would need to be recognized in addition to the bare results, and even then it would be unclear just what should be concluded unless the risk assessment is particularly explicit on the way it relates to reality or to some defined modification thereof.

We now consider the possibilities for risk assessment more closely targeted on reality, and the alternatives of nominal assessments, which can be more clearly defined, but which may bear tenuous relationships to the quantities which we would really like to manage.

2.1.2 Prospects for rule based assessments

The concept of a rule based assessment, used here, requires a little preliminary explanation, prior to the main discussion of prospects.

The concept of a rule is concerned with the substitution of reality by a nominal case or rule, normally selected to have some bearing on the reality of concern, and designed to make assessment more definite or tractable.

Examples of rule based assessments in nuclear analysis are:

i) Use of WASH-1400 source terms. Here a pessimistic source term is used rather than a realistic (possibly uncertain) one. If a safety target is achieved with the WASH-1400 source term, it is a fairly secure bet that it will be achieved with the actual source term.

ii) Denial of operator intervention within a set time (UK: 4 h). This rule denies the possibility of repair actions in an accident within a period wherein the repair actions might be rather difficult, and even more difficult to quantify. With respect to repairs it is a pessimistic rule, but the extent of the pessimism is quantified as yet. Applied to detrimental interventions it becomes an optimistic rule, with the error again unquantified. Either way, it denies certain aspects of the reality of operator intervention possibilities.

iii) Neglect of unidentified accidents.

This rather non-explicit rule has been used in most risk assess-
ments (WASH-1400 and the GRS phase A being exceptions) in that
there are not normally any contributions to assessed risk from completely unidentified accidents. The optimistic error involved with this 'rule' should decline with experience, but is quite difficult to quantify at present (the arguments over the conclusions of the Oak Ridge Accident Precursor Study exemplify the problem).

and, for illustration, a rule from a non-nuclear situation:

iv) The 'offside rule'.

This rule, in football, is used to deny the reality that the ball has arrived in the goal, so that the score of the game takes no account of such. Translating to an accident analysis context - it would be of little comfort in the event of an accident (ball in goal) to know that the risk assessment had declared the particular sequence to be 'offside' and thus outside the scope of the analysis, and of the design of preventive measures resulting from it.

Rule based assessments are normally used in conjunction with rule based criteria or guidelines, so that the guidelines are set together with the rules to be used in demonstrating their achievement. The severe accident frequency guideline of $10^{-6}$ for nuclear reactors is set in this context: along with it come various definitions of allowable system reliabilities, and the magnitudes of releases that constitute severe accidents. These rules may approximate well to certain aspects of reality, but they substitute something else for it, and to that extent introduce deviations from reality which may be unrecognised or unquantified.

Rule based assessment, particularly in regard to licensing, will probably be with us for some time, if not indefinitely. The success of such assessments in managing the realities which we would really like to manage will be largely dependent upon the degree to which the rules conform to reality. However, it is difficult to see how the interpolation of rules, as distinct from deliberate uses of approximations to enable the assessment process, can possibly enhance risk management, and it is clear that rules, poorly selected, may detract from it. Thus it is difficult to see any advantages in rule based assessment over the use of normal approximation methods in a realistic assessment. The latter method would of course create its own temporary rules for individual assessments, but would not be committed to any rules which were identified as serious misrepresentations of reality.

These problems with rule based assessment are suggested as reasons why quantities and towards management of the quantities which are of ultimate concern. Such a move cannot be immediate, in view of the investment in rule based analysis in the world, but the trend should be encouraged. Use of rule based assessment will always suffer from an ill-defined uncertainty about the relationship of the rule based quantities to those of actual concern, and these uncertainties will have qualitative aspects as well as the quantitative aspects which are inevitably common to all approaches.
3. THE SCOPE FOR RISK MANAGEMENT IMPACT ON COSTS

The performance of PRA incurs costs, and these costs must be justified by results in the improvement of risk management. There are several types of cost which could be affected by the use of PRA, and we look briefly at their magnitudes, since these magnitudes will give us a guide as to where cost impacts are available, and potentially sufficient to offset the costs of PRA and risk management exercises.

3.1 Actuarial costs of accidents

Risk management can affect the actuarial costs associated with accidents insofar as it can affect the expected frequencies. Most PRA studies have shown that the overall actuarial costs of severe accidents are dominated by onsite (plant) losses, rather than the less probable offsite losses, and thus a crude estimate of actuarial costs can be made on the basis of core melt frequency and cost. The former occupies the range $10^{-6}$ to $10^{-4}$ for most modern plants, while the latter is about £10^{9} in direct plant loss, with additional costs between £10^{7} and £10^{10} (this range based upon the effects seen after the TMI2 accident - eg the closure of THI-1 and the cleanup costs). These figures give a range for the annual actuarial costs of accidents:

$10^{3}$ to $10^{6}$ (extreme)

and a lesser range of:

$10^{4}$ to $10^{5}$

can be seen as a likely range for the actuarial costs for UK plants (based on a Sizewell core melt frequency of slightly less than $10^{-5}$ per year overall).

These costs are fairly small on the scale of reactor costs overall, and cost-effective risk management would only be possible on the basis of these costs if the risks were initially towards the upper end of the range. This situation reflects the fact that UK guidelines on risk are set at levels which have small associated actuarial costs.

3.2 Costs of safety design and operation

Because the safety guidelines are normally set below the levels which a straightforward application of cost-benefit analysis would produce, the costs associated with achievement of safety are much greater than the actuarial costs of accidents referred to above. Many of these costs are incurred in the initial construction of the plant, but some continue throughout the plant life, in maintenance and replacement costs, and in the levels of staffing required to carry out the safety related procedures. The elimination of ineffective procedures etc can impact these costs, as a result of a risk management programme after initial design and construction.

3.3 Plant unavailability costs

Safety related operations interact with plant availability, most notably when plant becomes inoperable because safety guidelines would be violated in the absence of repairs etc. Costs associated with plant outage are about £0.5M per day (£180M per year), and are thus at least an order of magnitude greater than the costs of safety related operations. Interactions of plant outage with PRA based risk management occur in such matters as operation with safety plant under maintenance, trip settings and their impacts on spurious trip rates, and operating rules concerned with conditions requiring shutdown or delaying startup.

3.4 Conclusions from cost impact discussions

The three areas discussed with respect to possible impact of risk management, viz:

- Actuarial accident risks
- Safety design and operation
- Unavailability of plant operation

are associated with quite different orders of magnitude in costs.

The results of PRA based risk management in reducing risks are associated with rather small costs, and PRA is least likely to be cost-effective in this capacity, although this has been its traditional role. Costs associated with safety related design and operations (about equal plant lifetime costs for each) are considerably greater, and provide reasonable scope for cost-effective impact of PRA based risk management, but the greatest impact of such management could be felt in the matter of plant availability for generation, since the associated costs are by far the greatest of those which can be affected by efficient risk management.
4. **POSSIBILITIES FOR PRA BASED RISK MANAGEMENT**

The conclusions from the preceding discussions can be summarized as follows:

1. In order to provide information for risk management, PRA should estimate the realities of risk, and avoid as far as possible the use of rules which may misrepresent them.

2. The cost-effectiveness of risk management is likely to increase as it impacts the larger associated costs of projects.

3. The ordering of associated costs is:
   - Actuarial accident costs (lowest)
   - Safety design/operation costs
   - Plant unavailability costs (highest)
   - and there are order of magnitude differences between each.

The overall deduction from these is that PRA should be aimed at relating risks to the above three cost related matters in priority order, and that it should do so via the realistic assessment of risks, rather than notional rules, except where those rules are seen to be good approximate representatives of risk realities. We now consider briefly the ways in which PRA could be used to address these issues.

4.1 Risk management for plant outage situations

Although a considerable amount of groundwork can be laid beforehand, management responses to plant outage situations must be on timescales of a day or less, requiring methods much faster than the traditional PRA methods. As it would not be feasible to anticipate all the outage situations which might arise, this would entail the use of a risk or reliability model for the plant, into which the current situation data could be fed, and from which some assessment of the plant reliability would emerge. This could then be used to determine whether or not startup could occur in various conditions which might fall short of ideal conditions. Similar processes could be applied to determine whether or not current degraded system conditions demanded immediate plant shutdown or power reduction (assuming of course that the conditions did not amount to a trip condition).

The reliability model (or risk model) would need to be as comprehensive as was consistent with the timescales of its use (circa 1 day or less). Supercomponent plant models, such as those used in the WCAP 9991 analysis of Sizewell B, would probably be suitable for this purpose. They could address the current probability of core melt given the safety system conditions, and could incorporate some crude eval-

4.2 Risk management for design of systems and operations

This aspect of risk management is derivable from the more traditional, extensive PRA studies, performed over long periods during the plant design and construction. These studies also have an input to the short term management of outages referred to above, in that they contribute to the risk and reliability model and the aspects of associated decision making which can be anticipated prior to outage situations.

The risk management could be derived from the risk output (at any selected stage) from PRA, and would be based upon identification in the PRA of the most critical features of plant design and operation in producing risks. These features would need to be identified by realistic risk assessments, as described in section 2 of this paper.

The features which can be addressed by PRA in this process include the major features of the design, quality requirements at the procurement and construction stages, and ground rules for operations. PRA can indicate, subject to the inevitable uncertainties in these matters, the items and areas upon which efforts and expense should be concentrated, and conversely, those in which expense can be spared on account of low importance to safety. However, these PRA based processes should be cogniscent of plant availability matters, as some items with little risk importance, such as conventional steam plant items, may have great influence on plant availability, and thus economics. As availability is associated with the greatest economic impact, such matters should not be neglected in the overall process.

4.3 Risk management for reduction of accident frequencies

Although there is a sense in which any risk management process is concerned with the reduction of accident frequencies below levels which might otherwise arise, this section addresses the specific issue of ALARA reduction of frequencies below some absolute levels determined to be necessary regardless of other considerations.
PRA results, via their identification of the causes of risk, are able in some cases to identify causes which can be easily and inexpensively eliminated, even though the associated risks may already be less than the absolute requirements.

This particular aspect of risk management is, however, unlikely to be cost-effective alone in view of the already very low levels of risk produced by the UK safety design guidelines, and is better seen as a process which can be carried on in conjunction with the management of design of systems and operations.

4.4 Summary of Possibilities

The ability of PRA to identify and quantify the causes of risk opens up several possibilities in risk management, and its interaction with design and operations. The viability of these possibilities is consequent upon the potential cost impacts, and this implies that risk management aimed purely at risk reduction below already low levels is not likely to be viable if conducted in isolation. However, the use of PRA results to indicate priorities in design and operational aspects is equally possible, and likely to be cost-effective, in view of the very small proportional cost impact required to pay back the PRA effort involved.

Uncertainty in PRA results, mentioned previously (section 2) will make the management tasks more difficult than they might be otherwise, and may for some time limit the possibilities of PRA based risk management to fairly crude and approximate levels. This matter is discussed in more detail next.

5. ANTICIPATED PROBLEMS ARISING FROM PRA UNCERTAINTIES

PRA based risk management will in its simplest forms involve the comparisons of risks (or reliabilities) for different situations, one of which may be the 'current' situation, or base case, and others of which may involve other possibilities, such as design and operational changes, changes to equipment specifications, or different decisions in the short term reactions to plant outages. In general, all the PRA results for the comparators will be uncertain, and there may be limited correlation between uncertainties for each.

We look now at some of the types of uncertainty which may arise, and discuss the requirements for making decisions based upon results which contain them. Decisions have to be made anyway, so the issue is not whether or not decisions can be made, but whether or not PRA could provide any useful input to those decisions. In order to be useful, the PRA input would need to be found superior to judgements based on less detailed views or pre-set guidelines, since these would normally be used in its absence.

5.1 Systems Analysis Uncertainties

Systems analysis uncertainties are normally dominated by reliability uncertainties attributable to one of:

- Dependent failures
- Operator error

and these have proved much more difficult to quantify than the reliabilities which could be calculated from independent component data alone.

The problems involved in the use of PRA results in systems analysis can be illustrated by considering the matter of common mode failure of redundant safety systems, as an example of several issues which suffer from difficulties in parametrisation. The standard methods of analysis of these in the UK have centred around beta factors or system cut-off values, neither of which relates to much of the specific detail of the systems under analysis. Therefore it is very difficult to relate any proposed change in a system to an effect on its reliability, assuming that the system remains redundant and generally of high quality. For, example, the reduction of a 4-train system to a 3-train system would have an apparently negligible effect on its common mode (and overall) failure rate according to some current methods, simply because the methods of cut-off and beta factor cannot discriminate between the two cases. Even when methods can discriminate (e.g. the Atwood method), the uncertainties in both results far outweigh the differences.
This particular problem, which is very important in systems analysis, illustrates a general problem of uncertainty which is associated with a lack of relationship of an assessment to the content of the system being analysed. The common-mode cutoff is the clearest example of this, but it arises in many other situations, such as operator action and quality assurance, where again there are no parameters of the situations which relate directly to the assessment quantities. What is needed here is some incorporation of a parametric method (at least) whereby the beneficial or detrimental effects of certain system changes, agreed to exist by a very wide consensus, can be fed into a PRA mechanism. It is true that the initial quantification of the parametrisation of system quality/quantity may rely heavily on judgements, but at least these judgements would be organised, and the effects in the right directions rather than in none. Without some such method, neither PRA nor any other quantifiable procedures can address such issues as:

- The level of redundancy required in a system
- The type of QA to be applied to components
- The level of search for systems interactions

and yet these are all recognised as important issues for safety system costs and performance.

Given some such methods as the above, discrimination between different possibilities becomes possible. Risk management can live with uncertainty, but cannot live with lack of discrimination between different possibilities. How it would live with uncertainty in this area is now discussed.

Given that discrimination is possible between different system possibilities (levels of QA, maintenance periods etc.), there remains the problem of decision under uncertainty. This uncertainty is likely to be expressed as some range of accident probabilities, and it will only rarely be possible to define any definite characterization of the uncertainty, such as a mean, distribution etc. Although some scheme based on judicious treatment of 'best estimates', upper limits etc. may seem very arbitrary, it is normally found to be less arbitrary than alternatives which do not even address the issue of uncertainty ranges. This matter of uncertainty is not therefore seen as a problem peculiar to PRA results - indeed is is less of a problem because at least some of the aspects of uncertainty are revealed in PRA, whereas all may remain hidden in other approaches to decisions. One has of course to believe that more knowledge leads to better decisions, but that is a matter of philosophy which I do not discuss further here.

5.2 Phenomenological Uncertainties

Major phenomenological uncertainties occur in two distinct areas of PRA: design basis LOCA analysis and post-core-melt analysis. The former have traditionally been smothered under pessimistic assumptions, so that traditional analysis (for LWR's) has been concerned with events at or beyond the fringes of reality in the LOCA area. In order to bring reality back to the assessments, some of the past work in the LOCA area would need to be undone, so that the LOCA's which may actually produce risks are analysed. Analysis of these LOCA's may lead to rather different views on priorities for safety system responses, and uncertainties involved may become larger than we have been used to in traditional analysis. However, the uncertainties will be favourably one-sided, and one can see little but advantage coming from analysis of them.

Uncertainties in post-core-melt situations are difficult to quantify, and are important in determining risk, if not the frequency of core melt. However, as pointed out earlier, core melt itself would normally dominate the actuarial costs of accidents, and risk management at this level, coupled with some approximate recognition of the differences in risk from different core melt sequences, would greatly reduce the importance of these phenomenological uncertainties, without a corresponding reduction in potential cost-effectiveness of the risk management process. Furthermore, the post-core-melt analysis, although it suffers from large uncertainties, does not suffer to the same extent from the lack of discrimination which would undermine risk management.

5.3 Discussion

Uncertainty in itself is not seen as a major barrier to the use of PRA methods in risk management, as the PRA process merely recognizes uncertainties which are there anyway, and will afflict whatever process of management is used. More serious in PRA at present is the lack of discrimination in assessment in areas where there is general consensus on the directions, if not the associated magnitudes, in which discrimination should be made. In order to be justifiably used, PRA methods must at least incorporate the judgemental discrimination which is available in other methods, so that agreed important aspects of systems and safety can be recognised in its analysis.
CONCLUSION

The foregoing discussions have ranged over several aspects of the possible use of PRA as a cost-effective risk management method. The principal conclusions of these discussions have been:

1) Cost-effectiveness will be greatest where PRA interacts with greatest plant costs. These are, in descending order:
   - Unavailability costs
   - Safety design and operation costs
   - Actuarial accident costs

Interaction with the first would be on a short (plant outage) timescale, and would be based upon analysis of interaction with the second over a protracted timescale. PRA concerned with the third alone was considered unlikely to be cost-effective.

2) Although there would still be a need for some PRA related to notional, rather than actual risks, a trend towards more realistic assessment of risks, disposing of conservative modelling, was seen as beneficial to risk management. Rules concerning assessment of notional situations may distort results and could not in compensation reduce uncertainty, which fundamentally underlies the whole subject area.

3) In some important respects, such as those concerned with QA and dependent failures, PRA has not achieved the level of discrimination available in other, judgemental methods. The achievement of this level is required for PRA to be used in preference to the more traditional judgemental methods in these areas.

The overall answer to the title question 'Can PRA Pay' is positive by implication in the foregoing discussions, despite the shortcomings mentioned above and in the main text. The principal reason for this possibility (and likelihood) is the enormous disparity between the costs of performing PRA and the potential savings of even slight improvements in cost-effectiveness in the areas of plant availability and general safety design and operations. One additional day in which a major plant remained on-line when safety requirements might have kept it off, would roughly repay the costs of a PRA-based process which could help to achieve this.
Regulators perspective of PSA as an Aid to NPP-Management

Peter Michael Herttrich

Bundesministerium des Innern
D 5300 Bonn 1
Federal Republic of Germany

CSNI Workshop on
PSA as an Aid to NPP Management
Brighton May 20-23, 1986

Regulators perspective of PSA as an Aid to NPP-Management

Introduction
To discuss the use of psa as an aid to npp-management from a
regulators perspective means to discuss the future role of psa
in supervisory procedures for operating plants.

My personal view:
- The systematic application of psa-approaches has the potential
to become a powerful investigative tool and information system
for safety- and risk-management of operating nuclear power
plants.
- The development and implementation of a psa-based safety- and
risk-management is at first the task of the plants-operators.
- PSA can today be considered as a well established, mature approach
to the safety review. So the duty of the regulatory authority is to
monitor, if operators make wise use of psa to manage the
safety of their plant. If this is not the case adequate regulatory actions must be taken.

The commitment to nuclear safety

Nuclear safety is achieved, if:
- normal operation and accidents give not rise to levels of
  exposure beyond respective limits
- severe accidents with unacceptable consequences for man and
  environment do not occur.

This is the real safety goal.

If a specific npp fulfills this safety goal can finally only
be decided at the end of the plants lifecycle. The commitment
to the pursuit of optimal safety precautions must be seen
from three different perspectives:

...
a look forward, to ensure that the precautions taken give acceptable high confidence that the real safety goal will be achieved

a fictive look back: imagine risk turns into consequences, a serious accident occurs; then anyone responsible for the safety of that plant must be able to justify looking back that all available and reasonable measures had been taken to prevent, to curtail or to mitigate the accident.

an overall perspective: the nuclear option will survive only very few severe accidents.

In this sense the regulatory authorities have to defend the real safety goal. If PSA offers new chances for the successful safety- and risk-management, they are responsible to ensure, that these chances are taken.

Regulatory Decisionmaking

Most regulatory authorities have chosen to rely to a very great extent on regulations to ensure public safety. Regulatory requirements are based on the so called deterministic approach, which can be characterized as follows:

To ensure, that the overall plant design is acceptable from the safety point of view

an overall safety approach is established as basis and reference for detailed requirements on lower levels (defence in depth, radiological criteria, necessary design features and safety functions)

- adequate safety of passive systems and components is achieved by conservative assumptions and adequate safety factors laid down in codes and standards

- adequate safety of active systems is achieved by prescribed reliability engineering concepts as for example:
  redundant design of safety systems (single failure and repair criterion)
  avoidance of intermeshed systems
  physical separation of redundant systems
  diverse design of redundant systems
  inherent safety principles
  fail safe principle

- adequate protection against events, especially against design basis accidents, has to be proved by event-sequence analyses under given assumptions:
  initial plant state and boundary conditions
  performance of active or passive systems as designed
  assumption of failure of a required safety function, if it has not been explicitly designed against the consequences of the given impact.

The advantage of the deterministic approach is to simplify and stabilize the design and licensing procedure. For a complete deterministic concept it should be possible to assume, that if a NPP is designed according to all deterministic requirements, then it is safe enough to be licensed. In practice the deterministic requirements can in principle be not complete, so that a measure of judgement is always involved.

The deterministic approach has served its purpose well. Nevertheless there are different issues, insufficiencies or limitations where the current practices of investigating and deciding nuclear power plant safety matters have been and will continuously be improved by using advances in the state-of-the-art in safety assessment methods, as for example probabilistic approaches.
So it is a current practice that PSA's are used during the design-phase and licensing procedures to:

- review the safety design for weakpoints
- demonstrate a sufficient reliability of systems important for safety and a balanced design.

Licensing decisions are based on conditional safety prognoses.

In the end, the regulatory decision to grant an operation licence is founded on a prognosis of the plants safety performance. This prognosis must be understood as a conditional prognosis because many conditions and assumptions must be made:

- the plant is constructed and operated as specified
- serious human failures can be prevented
- all safety-important initiating events and phenomena are in principle known
- scientific-technological knowledge and design principles have been applied correctly
- very remote initiating events or phenomena need not to be considered for the safety-design.

Technical experience has shown, that if accidents occur, then usually one of these conditions has not been fulfilled. Safety or risk is a matter of hardware, software and people and the specific way they interact. This is a very complex management task, for which the best available management information systems and managements techniques must be used.

Characterization of probabilistic approaches to safety decision making

Two different approaches have to be distinguished: First: the application of techniques of probabilistic safety analysis as an investigative tool to analyse the safety performance of the overall plant design or of components or systems under all events that the plant may be subjected to, taking into account a variety of initial or boundary conditions as well as further uncertain influences as for example human errors.

- a full scope probabilistic risk analysis (PRA) of level 1, 2 or 3 using NUREG CR-2300 terminology;
- a more or less extensive reliability analysis for a safety function or for the performance of the safety system given a special initial event and to assess the probabilistic that the plant will stay within the design limits.
- an investigation of special issues, as common mode failures of highly redundant systems or special transients or applications for special tasks as the evaluation of operational experience or the planning or evaluation of reactor safety research.

Applications of these types offer very useful engineering insights, assessments of the relative safety importance of different safety functions, special design features or operational modes and estimates of frequency and consequences of accident sequences.

Second: the application of probabilistic criteria to justify safety related decisions. Such criteria could be:

- absolute quantitative safety criteria as limits for acceptable mortality risk, dose-frequency limit curves, core melt frequencies, quantitative reliability requirements for system functions or
relative safety criteria as "balanced design", relative contributions to unacceptable plant conditions, subsystems unavailability should not determine systems unavailability or risk oriented gradation of the stringency of safety requirements.

The first approach will be called the technical-pragmatic, tool oriented approach, the second the normatively, goal oriented approach.

Comparison of deterministic and probabilistic approaches to safety decision making

The decisive factors for the weight to be given to deterministic and probabilistic approaches in npp-safety-decision-making are the respective strengths and weaknesses of both approaches.

Deterministic principles

- can easily be applied and verified. They result in inherent safety - and reliability-features.

- enable safety decision making even under limited knowledge of phenomenology and of plant response to transients and accidents.

- overcome uncertainties or deficiencies in knowledge by conservatism.

- can in principle not distinguish between more or less reliable systems or more or less frequent disturbances (demands for safety functions).

- offer no information about necessary test intervals and acceptable repair times.

- result generally in unbalanced design in both directions.

Probabilistic analyses

- describe the relative safety importance of systems and structures and the level of safety achieved by a given design.

- identify unbalanced design features and allow to streamline safety functions

- help to identify and remove weaknesses or design deficiencies.

- assess possibilities and limitations of safety improvements/risk reduction.

- help to optimize test-, inspection- and maintenance- procedures

- make it possible to compare different design alternatives.

- require much information on the details of system design and data bases for the frequency of initiating events and failure rates, which often put a full scale application out of question.
- can lead quickly to models too complex to be analysed.
   Simplifications are necessary which imply similar drawbacks
   as the deterministic approach.

- need specially trained expert-teams.

Both approaches have different advantages, which can efficiently
complement one another. With increasing knowledge and experience
about the operation and safety performance of npps probabilistic
analyses gain increasing importance, because they enable more
precise information about the safety characteristics of a
specific plant and its operation.

It can be stated that the real advances in npp-safety-assessment
and decision making in the past years have been achieved by a
combination of deterministic and probabilistic approaches.

Goal oriented or tool oriented approach to the use of psa

Two different ways to implement a more systematic use of psa
into safety decision-making have been described above:

- the technical-pragmatic, tool oriented approach
- the normative, goal oriented approach.

Quantitative safety goals in terms of risk limitation have
been investigated and compared with results from full scope
PRA's. It can be concluded, that the estimated risk of modern
plants to the public is not too high. Therefore there is no
reason to develop new quantitative safety goals to define an
acceptable low risk level. The level of acceptable low risk
has implicitly be defined by the level of safety provided
by recent modern npps according to the actual knowledge.

Much work has been spent on theoretical investigations in
risk perception, public acceptance, risk averlon, risk comparisons
and so on. I think this will never come to an really useful end:
there are too great uncertainties around acceptable risks and
estimated risks.

A PRA-study can only be a snapshot of the safety level of
a plant under the specific information available and assumptions
at a certain time. But the frequency of initiating events and
the reliability or availability of systems important to safety
can be influenced positively or negatively by many different
factors or must be reassessed because of new scientific-
technical results or operational experience.

So the name "quantitative safety goal" in terms of individual
or collective risk or core melt frequencies is misleading. They
can not be a complete substitute for the real safety goal
mentioned before. Low risk estimates are a necessary prerequisite
but not a sufficient condition for the successful management of
a specific plants safety. The quantitative safety goal approach
does not reach beyond the level of a conditional prognosis. But
the real safety goal can only be achieved with successful
safety- and risk-management during operation.

Public acceptance of the peaceful use of nuclear power is not
an issue of quantitative safety goals or low risk estimates but
it is an issue of credibility and confidence in the successful
safety- and risk-management of nuclear power plants.

The pragmatic tool oriented approach is convenient to
develop a systematic use of psa for future safety decision-

Supervisory procedures

Because licensing decisions can only rely on conditional safety
prognoses the licensees are submitted to a supervisory procedure.
The duty of the competent authority is to monitor and control
the effectiveness of self-regulation of safety matters practiced
by the operator within the framework of license conditions and
all documents, to which the licence refers. Main objectives
of supervisory procedures of the authority are to ensure:

- that the plant is operated, maintained and repaired in accordance with all relevant requirements and conditions
- that parameters important for nuclear safety and radiological protection are continuously monitored and appropriate measures are taken to keep safety margins high
- that operational experience is evaluated and used for improvements and optimization
- that new assessment methods and new safety relevant information is used for monitoring the safety status of the plant, for the elimination of possible deficiencies, for reasonable improvements or for the optimization of the overall plant safety.
- that changes in operation or modifications in design are compatible with the actual plant status and safety requirements

Authorities are empowered to control npp-safety by more or less restrictive means, that can reach from reports or recommendations up to the withdrawal of the licence.

The decide about adequate or necessary supervisory actions different procedures for information-collection and evaluation are practiced:

**Plant specific activities**
1. Inspection
2. Test and maintenance programs
3. Regular report
4. Special reports
5. Review of personal qualification and training
6. Environmental surveillance Programs
7. Special investigations

---

**Activities independent from single plants**

1. Central collection and evaluation of operational data and operational experience
2. Review of actual research and development
3. Stimulation of new research.

Enormous amounts of information have to be reviewed for the careful selection of what is important or necessary for safety and which improvements for safety seem to be reasonably achievable.

There are many practices that have served these purposes well. But the evolving maturity of PSA-techniques allows now to integrate proven practices into a more systematic and comprehensive approach to ensure successful safety and risk management by the operator.

**The different roles of the parties involved**

Although different parties: authorities - utilities - industry - experts are involved in this management process, the practical management of safety and risk for a npp can only be performed by the operating utility. So the involvement and participation of authorities or other organisations must not diminish the responsibility of the licensee.

But all parties share a common responsibility for achieving the real safety goal. This requires the cooperation of complex organisations, also a complex management task. Cooperation-effectiveness -credibility can easily become competitive objectives, what can lead to suboptimal or even irrational actions.

Utilities and Vendors have to accept that authorities must strive for optimal safety precautions. There can be no cut-off for safety oriented thinking. Authorities have to accept that they are not the plant operators and that safety cannot be regulated against better arguments. ...
I think that the systematic application of PSA can reduce unnecessary conflicts giving more rationality and transparency to decision-making.

It simplifies the communication about safety issues between parties involved. It can help to treat safety issues according to their relative importance and to identify commonly acceptable solutions.

**Cost-benefit criteria**

Formal cost-benefit criteria for safety decision-making are not very useful. They should only be used if all rational approaches have not worked. Once a safety problem has been identified there are usually many different solutions. They have to be identified, analyzed and evaluated. I think it is more rational to negotiate to pros and cons of the different solutions within the given technical context than to associate theoretically estimated doses and costs with them. These data usually give very few information about the real consequences of such a measure for the safety- or risk-management of the plant. This is a further reason for the systematic implementation of PSA as an management tool:

As an investigative tool it offers intelligence to identify problems, as a design tool it supports the development of alternative solutions and as a decision making tool it allows to compare and decide alternatives.

**Utility experiences with PSA as a management tool**

Different utilities have already started to use PSA in this way, so that I am convinced that PSA has the potential to become an integrated approach to NPP-safety-and risk-management.

Concepts for this approach have been developed as "living PRA Model", "Integrated living Schedule Program", "Systematic Reliability Assessment Program". First experience has been gained, but I think the concept is still in the "definition phase". What is needed now is an "evaluation of PSA as a management tool". This must be done by practitioners that have first hand experience with safety- and risk-management of a npp, i.e. operators, technical consultants, R & D institutions, in dependent experts that are adopted by the authorities. It makes a difference if a PRA should be performed for a best estimate of bottom line risk or if PSA-information should be available for concrete, practical safety- and risk-management tasks.

**Background and guidance for a PSA-based management concept**

Let me finally survey some issues that give background and guidance for the development of the PSA-based safety- and risk management concept.

1. **Management theory**

   The first point is quite general, but stimulating: If PSA should be used as a management-technique, results of management- and organization theory should be applied. From a management technique it must be expected, that it:

   - simplifies the duties of the responsible managers
   - is flexible and highly adaptable to changing boundary conditions
   - is self-regulatory
   - is economic and
   - proofs measurable success and significant benefit.

   A PSA-based management concept must be evaluated against these criteria.

   The specific design of such a concept can for example be deduced from:
3. Collection and evaluation of operational data

Fundamental questions to be decided are:
- which plant specific data should be collected in what form?
- how can the safety relevant information be extracted from
  the data to support engineering and operational applications?

There can arise a conflict, which data should be collected
and evaluated by central organisations working for the
authorities.

Here operators are afraid of too much information for the
authority. They argue, that a primarily statistical evaluation
of operational data is not sufficient. Preventive countermeasures
were only possible on the basis of a detailed engineering
analysis of the specific characteristics of systems or
components. This only could be performed by the utility.

On the other hand, there are good reasons for the central
collection and evaluation of special safety relevant operational
data by independent experts.

The most important is, that in the sense of a cooperative
effort to ensure safety, it is necessary that independent
experts are familiar with operational details for those areas,
that requires special interest and where only a broader data
base can help to understand what the actual performance
of the safety systems is. Furthermore data collected and
evaluated by independent experts are more easily accepted
by authorities, if they should be used for review purposes
under licensing or supervisory procedures.

4. Evaluation of abnormal occurrences and incidents

Two aspects are of special interest for the definition of
a psa-based management concept.
The first is that plant specific data bases and system logic models can make it much easier, to transfer operational experience from other plants to the specific plant, to assess the relative importance of the special event and to identify and evaluate possible consequences.

The second is, that plant specific precursor-studies can offer insights and guidance about areas, which are most important for successful safety- and risk-management and where improvements are most important.

5. Further management tasks, from which detailed requirements for the use of PSA as management tool should be deduced are:

- periodical tests and inspections
- the development of operational procedures
- the safety review of planned modifications of plant design or operation
- the training of personnel
- accident management
EXPERIENCES OF THE USE OF PSA METHODS AT THE TVO POWER PLANT

M. KOSONEN, A. PIIRTO and J. VANNALA
Industrial Power Company Ltd., 27160 Olkiluoto, Finland

T. MANKAMO
Avalon Oy, Ellipsikuja 3 B, 02210 Espoo, Finland

U. PULKKINEN
Technical Research Centre of Finland, Otakaari 7 B, 02150 Espoo, Finland

CONTENTS

1. INTRODUCTION
2. PLANT DESCRIPTION
3. TEST ARRANGEMENTS OF APWS
4. PREVENTIVE MAINTENANCE
5. CLOSING VALVE STUDY
6. SHUTDOWN RISK EVALUATION IN CASE OF DIESEL GENERATOR FAILURES
7. SHUTDOWN RISK EVALUATION IN CASE OF FAILURES IN THE RESIDUAL HEAT REMOVAL SYSTEMS
8. SUMMARY
APPENDICES

Paper to be presented at the CSNI workshop on 'Probabilistic Safety Assessment (PSA) as an Aid to Nuclear Power Plant Management'

Brighton, May 20-23, 1986
EXPERIENCES OF THE USE OF PSA METHODS AT THE TVO NUCLEAR POWER PLANT

The Industrial Power Company Ltd. operates two identical BWR units, TVO I and TVO II in Olkiluoto, Finland. The net electrical power capacity of both units is 710 MWs.

Technical Specifications set forth limits and operating conditions to operation of nuclear power plant for the protection of the health and safety of the public. So far the background has been mainly deterministic in defining the allowed operation times after a failure of a safety related component or system and has been based on engineering judgement. Because of the developed methods in reliability analysis and risk assessment it has become possible to evaluate different kinds of effects that failures really have. Reliability-based assessment can be used as a valuable aid to decision-making.

The probabilistic methods provide a systematic approach which can be used

1) to evaluate the additional risk during the presence of component failures in safety-related systems and

2) in case of specific failure combinations to compare the safety benefits of continued operation to the additional transient risks associated to the shutdown.

The applications of probabilistic approach began with studies concerning optimization of periodic tests and preventive maintenance during power operation. In the next step, the question of allowed repair times of failures in safety related systems during plant operations was undertaken for systematic treatment. The first study was concerned with the comparison of black out risks during continued operation with decided shutdown in case of diesel generator failures. This analysis served mainly methodological development purpose. The insights obtained encouraged to continue with an analysis of the systems for residual heat removal.

Parallel method development is continued in the joint Nordic project "Risk Analysis and Safety Philosophy", which is conducted during 1985-1989 as a part of the research program of NKA (Nordic Liaison Committee for Atomic Energy).
2. PLANT DESCRIPTION

TVO nuclear power plant is operated by Teollisuuden Voima Oy (TVO, Industrial Power Company Ltd.) The plant is located at Olkiluoto on the western coast of Finland and it consists of two identical BWR units, TVO I and TVO II, supplied by ASEA-ATOM, Sweden. The net electrical power capacity of both units was originally 660 MW, but since uprating in 1984 it has been 710 MW. The first criticality of TVO I was reached in July 1978 and the first criticality of TVO II in October 1979. The annual capacity factors of both units are listed in Table 1.

\[
\begin{array}{|c|c|c|}
\hline
\text{Year} & \text{TVO I} & \text{TVO II} \\
& (\%) & (\%) \\
\hline
1979 & 59.9 & - \\
1980 & 73.9 & - \\
1981 & 79.4 & 60.8 \\
1982 & 87.3 & 79.9 \\
1983 & 81.8 & 88.7 \\
1984 & 90.7 & 87.2 \\
1985 & 87.4 & 87.4 \\
\hline
\end{array}
\]

2.1 Design features of safety-related systems

Safety-related systems at TVO I/II are divided into four redundant parts separated from each other. The principle of using four half-capacity (4 x 50%) systems is applied in all important safety functions. Normal performance of two out of four subsystems is sufficient to cope with possible incidents and accidents. The redundant circuits of safety-related systems are assigned to two main groups, which are located in physically separated areas. Within these areas a separation by distance or by means of barriers is used between the redundant parts. The main flow diagram of the power plant is presented in Appendix 1.

2.2 Technical specifications

Technical Specifications give, in the event of faults, the longest repair times depending on the kind of faults. During these repair times the power operation is allowed to continue, but if the repair of a fault is not possible or if the repair time is or will be exceeded, the operational condition have to be changed to a safer condition. Usually this means cold shutdown of the power plant. For safety-related systems the following repair times are given:

- With one out of four subsystems inoperable, power operation may continue 30 days without restrictions
- With two out of four subsystems inoperable, power operation may continue 3 days without restrictions
- With three or four subsystems inoperable, cold shutdown has to be reached within 24 hours

For systems which have not been credited in accident analyses of PSAR, the following repair time is given:

- With a system failed so, that it does not fulfill single failure criteria, power operation may continue 7 days without restrictions.

The auxiliary power system is divided into safety-related and non-safety-related systems, in accordance with the requirements on the process systems to be supplied with power. The schematic electrical diagram is presented in Appendix 2. Power is normally taken from the generator busbars across two plant transformers, but as a backup there is a startup transformer connected to the 110 kV grid. These two power sources are independent.

The distribution network is divided up into four separate sections. This division is consistently pursued for the power supply to motors, control equipment, etc. throughout the power plant. Four diesel generator units provide onsite standby power supply, and battery-backed systems supply no-break d.c. power and priority a.c. power across rotary converters.
The auxiliary feedwater system (AFWS), like other safety-related systems, consists of four redundant trains. The study was aimed at investigating the sensitivity of the AFWS unavailability with respect to the interval of the periodic tests and the test scheme as a whole.

The study was limited to the unavailability of the auxiliary feedwater function on demand (start-up of the system only). The pump cooling systems and the power supply systems were not taken into account.

This application was chosen because of the interest to analyze, whether part of the rather frequent periodic tests could be removed. The basic test scheme and two main alternatives, presented in Table 2, were analyzed. In alternative I the interval of pump tests is increased from one to two weeks, but this is intended to be compensated by combining valve tests with pump tests. In alternative II the testing is further reduced to four weeks interval.

The mean unavailability of the AFWS with all three test schemes was calculated by using the "q - A t" model for the components, which is defined in Chapter 5. The parameters for each component were estimated on the basis of operating experience of TVO I and TVO II, which was rather sparse at that time: in 1981 altogether 5 reactor years. The lambda-part could be derived rather reliably from the failure data, but the q-part had to be assessed solely on engineering judgement. The methodology used has been described in detail in Refs. 1/1-3/.

Also the contribution of repair periods was calculated. On the mean unavailability the repair periods have, however, only a small influence.

The minimum mean unavailability was obtained in alternative I (see Fig.1). This can be explained by the fact, that in the basic scheme the pumps are tested unnecessarily often, but the isolation valves in the injection lines with so long interval, that shortening it from four to two weeks is beneficial. However, the differences are still rather small between the options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Train</th>
<th>Week 1</th>
<th>Week 2</th>
<th>Week 3</th>
<th>Week 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic scheme</td>
<td>A</td>
<td>P</td>
<td>P</td>
<td>PV</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>B</td>
<td>P</td>
<td>P</td>
<td>PV</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>C</td>
<td>P</td>
<td>S</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>D</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>S</td>
</tr>
<tr>
<td>Alternative I</td>
<td>A</td>
<td>PV</td>
<td></td>
<td>PV</td>
<td></td>
</tr>
<tr>
<td></td>
<td>B</td>
<td>PV</td>
<td></td>
<td>PV</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C</td>
<td>PV</td>
<td></td>
<td>PV</td>
<td></td>
</tr>
<tr>
<td></td>
<td>D</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alternative II</td>
<td>A</td>
<td>PV</td>
<td></td>
<td>PV</td>
<td></td>
</tr>
<tr>
<td></td>
<td>B</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>C</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>D</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

P= Test of the pump
V= Test of the valves in the injection line
S= System test of the whole train with injection into the primary system

In trains A and B the system tests (S) are carried out once a year only (to minimize thermal stresses).

Reducing the testing to four weeks interval according to alternative II does not result in any substantial increase in the mean unavailability.

The results proved to be quite insensitive with respect to the uncertainties in data, especially for the "q - A t" model parts. Considering these results now with better knowledge of data, the qualitative results are still fully valid, and even the quantitative results when considering the relative point of view.

To conclude, in alternative I the tests are allocated in a balanced way between pumps and valves. The results were used to support the decision of rearranging the test scheme, which currently is almost identical to alternative I.
4. PREVENTIVE MAINTENANCE

The purpose of preventive maintenance is to detect and repair in good time defects which could cause, when developed further, failure of or damage to equipment.

Preventive maintenance normally requires that equipment is taken out of operation and isolated, because of worker safety, before service or inspection can be done. The allowed repair times according to the Technical Specifications are not intended for any planned maintenance activities in safety-related systems. The repair times are determined supposing that failures are incidental. Maintenance is therefore usually carried out during a refuelling outage.

Preventive maintenance during power operation could be possible for standby system, for example for certain safety-related systems. The disconnection of one out of four trains does not contradict the deterministic safety criteria. In this respect it would be an advantage if part of the work could be done at another time than during refuelling outage. Work can be performed more carefully and without hurry using company’s own employees. The quality of work will be better. More event apportion of maintenance times can also improve average availability.

Because the approach was new, the consequences were considered carefully. The influence of preventive maintenance during operation on the unavailability of the safety-related systems was estimated and compared to WASH-1400 (see Fig. 2). The increase of unavailability was rather small. On the other hand, it can further be decreased by grouping the preventive maintenance activities in different systems in such way that functional dependencies between the systems are taken into account. Thus the unavailability of the safety functions remains at acceptable level.
Preventive maintenance during power operation has been in practice since 1981 and it has shown good results. It has helped to keep component failure rates down and, with strict maintenance time limitations, also the unavailability of safety related systems at very low level. Thus the condition of equipment ensuring safe operation of nuclear power plant, is always good and safety margins are wide. This maintenance praxis has also economical significance, since the length of the refuelling outage can be kept somewhat shorter.

![Graph showing percentages of containment vessel spray system, core spray system, auxiliary feed water system, and diesel generator systems](image)

Figure 2. Unavailability (%) due to maintenance (one out of four subsystems unavailable). A comparison between WASH-1400 and TVO praxis.

5. CLOSING VALVE STUDY

The operational and failure data of closing valves related to the containment isolation function has been collected and analyzed in order to study the applicability of a standby component failure model /6/.

The failure were classified into the following categories:

- LC, latent critical failures
- LM, latent noncritical failures
- MC, monitored critical failures
- MN, monitored noncritical failures

Monitored failures were modelled with constant failure rate. The latent critical failures were assumed to contribute according to the model

\[
u(t) = q + (1-q)(1-e^{-\lambda t})
\]

(5.1)

\[= q + \lambda t \quad \text{if both } q \text{ and } \lambda \leq 1\]

where

- \(u(t)\) = latent instantaneous unavailability
- \(q\) = time-independent part
- \(\lambda\) = standby failure rate
- \(t\) = time elapsed from the previous test or other demand

The probability of latent noncritical failures is also modelled with equation (5.1).

The total unavailability of the valves was dominated by latent critical failures. The failure probabilities estimated directly from data and those calculated with equation (5.1) are presented with 90% confidence bounds in Fig. 3. The fit of model is based on maximum likelihood model method which yields parameter values of \(q_{LC}\) and \(\lambda_{LC}\) given in Table 3.
### Table 3

<table>
<thead>
<tr>
<th>Failure category</th>
<th>Estimates of parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>LC, latent</td>
<td>$\lambda_{LC} = 3.7 \times 10^{-3}$</td>
</tr>
<tr>
<td>critical failures</td>
<td>$\lambda_{LC} = 5.8 \times 10^{-6}$ h$^{-1}$</td>
</tr>
<tr>
<td>LN, latent</td>
<td>no failures</td>
</tr>
<tr>
<td>noncritical failures</td>
<td></td>
</tr>
<tr>
<td>MC monitored</td>
<td>$\lambda_{MC} = 4.1 \times 10^{-6}$ h$^{-1}$</td>
</tr>
<tr>
<td>critical failures</td>
<td></td>
</tr>
<tr>
<td>MN, monitored</td>
<td>$\lambda_{MN} = 1.9 \times 10^{-5}$ h$^{-1}$</td>
</tr>
<tr>
<td>noncritical failures</td>
<td></td>
</tr>
</tbody>
</table>

These failure models and failure parameters estimates were used to optimize surveillance test intervals. The obtained theoretical optimum was in rather good agreement with the present test intervals, which have been chosen mainly according to practical engineering judgement (see Fig. 4).

![Figure 3](image3.png)

**Figure 3** The latent unavailability (critical failures) with 90% confidence bounds as the function of test interval of closing valves.

For the statistical treatment, valves were grouped in four groups according to the mean test interval.

![Figure 4](image4.png)

**Figure 4** The mean unavailability and optimum test interval of closing valves.
SHUTDOWN RISK EVALUATION IN CASE OF DIESEL GENERATOR FAILURES

Much interest has been devoted to the question of the allowed repair time in case of critical failures. The first approach was concerned with acceptance criteria for relative additional risk caused by repair periods /3/. It was soon noticed, however, that the consideration should be extended to the comparison of different decision alternatives of continued operation versus shutdown in case of reduced safety-related system availability.

The first study with this new approach was concerned with the failure combinations of the four diesel generators. The two possible decision alternatives and the respective event sequences resulting in station blackout are illustrated in Fig 5. The blackout is here defined as a loss of power supply to the feedwater system and to the shutdown cooling systems that endangers the core cooling. In the risk calculations the possibility to restore electric power within a given time is taken into account.

In this study quite a lot of work was concentrated on collecting empirical data on the loss of external power supply (all connections from the TVO nuclear power plant to the external grid). Special emphasis was put on finding out what is the probability of abrupt disconnection of the main generator in the case of a shutdown disturbance, and furthermore, what is the conditional probability of loosing the external grid given that kind of disconnection.

Figure 5. Operational alternatives and possible event sequences resulting in station blackout in case of double failures of diesel generators.
The results of the study were interesting and partly unexpected.

1) The risk associated to the repair time of 30 days with one DG failed is relatively small compared to the risk of the repair time of 3 days with two DGs failed.

2) If all four DGs have failed, it is a smaller risk to continue operation over the expected repair time of at least one DG (about 1 day) than to shutdown (as required by the current Technical Specifications), because of the relatively high disturbance probability associated with the change of plant state.

This study indicated that in this case the current Technical Specifications are not well balanced, and that new valuable insight can be obtained by use of the probabilistic methods.

The study was, however, concerned with limited, although important system part. In the course of the study it was realized that this kind of risk comparisons should be made at a higher level, at least at the main safety function level, preferably at the plant level.

7. SHUTDOWN RISK EVALUATION IN CASE OF FAILURES IN THE SHUTDOWN COOLING SYSTEM

The shutdown risk evaluation of diesel generator failures was extended next to the shutdown cooling system and other systems for the residual heat removal (RHR) function. The electric power supply was included as a support function.

The systems that could be used for RHR function are schematically presented in Fig. 6. There are three paths available for removing heat in shutdown state from the primary system to the ultimate heat sink (sea water).

7.1 Reduced model and data

In order to facilitate evaluations by developed component and sequence models, it is necessary to reduce system models as far as possible. The main reduction principle was modularization.

The calculations are based on the Minimal Cut Set (MCS) presentation of the failure sequences resulting in the loss of RHR function. Only sequences starting initially from the full power operation are considered. Restoration possibility of failed equipment or EPS has been taken into account. The available time for restoration in order to prevent the loss of core cooling function was assessed for different types of failure sequences. These times were determined by the critical limit of condensation pool temperature or by the decrease of the primary coolant inventory during blackout.

The component reliability parameters, repair time distributions, transient frequencies and other data were mainly inferred from the operating experience (about 10 reactor years). For the rare events, data from Swedish BWR plants was used as supplementary information.

The calculations have been done with the prototype version of computer program TeReLCO /7/ developed by Aviaplan Cy.

7.2 Important findings

Some results concerning the events where failures are detected in 721-712 lines (denoted as PL modules, see Fig.7.) are presented here.

The conditional risk frequencies for each failure combination are illustrated in Fig.8. The base risk for nominal full power operation is defined with the condition that no failures are detected and no maintenance disconnections in the RHR systems are present.
The risk frequency if shutdown is decided is presented in Fig. 8 for the case of double PL failures. The initial peak is mainly composed of the risk that one or both of the available PL modules will fail on demand. After about 10 hours from the shutdown the risk frequency drastically decreases when the capacity of one 721-712 line exceeds the residual heat production level.

The integrated risks for the operational alternatives and the expected number of failure situations are presented in Fig. 9. The following variables are used:

N.TL = Expected number of the specific failure situations over the plant lifetime (40 years)

N.LCO = Expected number of the failure situation prevailing longer than the allowed LCO time, i.e., single PL failure not being repaired in 30 days, and either of the two PL failures not being repaired in 3 days, respectively. In case of 3 or 4 PL failures immediate shutdown is required.

RCO.PE = Integrated risk per event (relative to the lifetime base risk) assuming continued plant operation over the repair time of PL module(s)

RSD.PE = Integrated risk per event (relative to the lifetime base risk) assuming decided plant shutdown promptly after the detection of PL failures(s).

Both risk variables are given as ratios with respect to the baseline risk over the plant lifetime (40 years).

In case of single and double PL failures the alternatives of continued operation and decided shutdown represent nearly equal risks. But in case of more failures the continued operation becomes significantly more favorable. This is due to the relatively high starting unavailability of the remaining 721-712 lines and the risk of losing EPS as a result of abrupt load disconnection during shutdown.

**Figure 8.** Illustration of the loss of RHR frequency in case of PL (721-712 pump line) failures

N: CO = Continued operation in case N PL modules are detected failed

SD = Shutdown decided
The absolute results are sensitive to many input parameters and model aspects. An example of sensitivity analysis where the failure probability of the 331-763-714 path (M331) is varied with a factor of 4 is presented in Fig.9.

At the present some refinements are being done in the quantification model. Proposed changes in the rules of the current Technical Specifications will be carefully evaluated. The validity of conclusions will be systematically verified by extensive sensitivity studies with the aim of obtaining adequate decision basis for possible changes.

Applications described here have supported test interval optimization of the main components in the AFMS and isolation valves for the containment. The implementation of preventive maintenance practice was also to a large extent dependent on the results of reliability analyses. The recent study is now under final evaluation with regard to conclusions. The results are likely to justify changes in the shutdown requirements concerning failures in RHR system.

The use of probabilistic methods for the verifications of technical specifications requirements looks very promising. Uncertainties are mainly caused by the lack of relevant data. However, the effects of uncertainties can be analyzed by use of sensitivity calculations. Typically, most of the potential conclusions are insensitive with respect to uncertainties.

Apparently, the periodic tests and allowed repair downtimes could be allocated in a better way, and an improved balance could be obtained both from safety and economy point of view. These kind of evaluations will be continued parallel to and on the basis of the PHA study that was started in 1985.
REFERENCES


Schematic electrical diagram.
ASPECTS OF QUALITY ASSURANCE FOR SAFETY MANAGEMENT
IN A NUCLEAR POWER PLANT IN OPERATION
FROM THE VIEW OF A UTILITY IN THE FRG

Dr. J.W. Weber
Kernkraftwerk Krümmel (KKK) GmbH
Geesthacht, Federal Republic of Germany
Abstract

Plants in operation constitute data and records which are of interest to the probabilistic safety assessment (PSA).

Performing functions are established which assure the compilation of data such as recordings on unavailabilities in safety systems, recordings on faults in the reactor protection system and the succeeded maintenance.

An internal authorization procedure safeguards that all aspects of plant and industrial safety as well as of radiation protection are observed.

The "display of core cooling systems" which gives an overall information about the status of the core and containment, especially in the case of emergency, is a further contribution to safety.

Modifications and maintenance in safety-related systems are of major interest. Therefore measures have been taken to establish a feedback of informations to those independent experts concerned with PSA.

A procedure of certifications is carried out every year to verify the current status of the plant in reference to the licensed requirements.

Finally, the quality assurance verifies the effective execution of the performing functions related to safety significance by means of a quality assurance programme.

1. Introduction

The operating license is given on the basis of quality characteristics, quality assumptions and quality requirements – see picture (1).

The electric utility has to safeguard the observance of these criteria by means of administrative and organisational structures with clearly defined functional responsibilities, by means of support and review functions and by means of the implementation of further steps of quality control and/or quality assurance.

Whatever step has been taken, it serves the purpose to verify that site activities relevant to safety are carried out within the limits that are established by the licensing process, i.e.

- preserving the quality of all components during plant lifetime,
- safeguarding the health and safety of the personnel
- providing for adequate training to plant personnel
- providing for the updating of manuals, procedures, instructions
- performing surveillance tests
- eliminating identified deficiencies.

The utility, however, has a legitimate interest in modifying those criteria which are too narrowly defined in the light of operational experience, such as to reduce the frequency of testing, if it is proved by experience of reliability.
2. Procedures of documentation and reporting

2.1 Plant Operating manual

The operating manual (containing 25 file folders with about 10,000 pages) is the only legal guideline for all operational activities under normal conditions, under anticipated abnormal occurrences and under accident conditions.

For the purpose of the probabilistic safety assessment the provisions of the operating manual concerning the necessary available numbers of safety- and safety-related systems during plant operation are of great importance.

Due to the interdependence between subsystems of the safety system great care has to be taken in controlling the state of availability for all associated parts of the safety system - see picture (2).

The prerequisite repair work at the service water system (VS) causes necessarily the removal from service of one redundancy each

- of the closed cooling water circuit (V2)
- of the associated low pressure coolant injection & decay heat removal system (TH)
- of the containment sump recirculation system (TS).

The diesel-generator FXD has to be removed from service inevitably because of the loss of service water (VS). Furthermore the high pressure coolant injection system (Y3) is declared as not being in service because of a supposed loss of auxiliary power connected with the unavailable diesel-generator (FXD). Therefore some armatures (especially isolation valves) have to be taken in their safety-related position.

The provisions of the operating manual describe clearly - as shown in columns (3), the permissible time which can be spent on corrective maintenance and what further actions have to be taken. The time available and the necessary activities depend, of course, on the number of redundancies not in service. At last the operating manual contains measures to be carried out, when maintenance was unsuccessful.

In the example the permissible maintenance time is fixed by 7 days, because one redundancy of the low pressure coolant injection & decay heat removal system (TH) is unavailable. Within 72 hours inservice tests of all other TH-redundancies have to be conducted. An unsuccessful maintenance leads to a power setback on low level.

Unavailabilitys of this kind are documented in the daily written report of the shift supervisor and are published monthly in the plant report about the operation experience of the plant.

2.2 Procedures of reporting

All events in a nuclear power plant such as

- operational inservice tests
- failures of essential units
- changes in the availability of safety- or safety-related systems
- modification and maintenance programmes
- changes in safety or safety-related equipment interlock
- changing of filter
- executed training and retraining programmes
- activity discharge at the stack
- startup and shutdown operations
- power cycling operations
- abnormal occurrences
- occurrences under accident conditions

are subject to reporting.
The events are documented in:

- daily reports written by the shift supervisor
- plant report -monthly published- on the operation experience of the plant
  - i.e. unavailability of safety systems
- reports on changes in the safety interlock system
- report on maintenance
- application for modification
- equipment-control log of the reactor protection system
  - faults and defects in the reactor protection system
- significant-event-report addressed to the Association for Reactor Safety
- release documents of the work authorization procedure
- life duration records
- refuelling period report emphasizing
  - maintenance and modifications
  - shutdown period inspections
  - analysis of radiation exposure
  - effectiveness of radiation safety measures and their feedback
- report on the operation experience published per annum emphasizing
  - systematic failures
  - insufficient maintenance with repeated failure
- Annually published report addressed to the Reactor Safety Commission
- Annual progress report about the state of the art.
  - new requirements from safety guidelines
  - feedback coming from operating experiences made in other nuclear power plants

2.2.1 Records of unavailabilities in the safety system

The scale and depth of recording can simply be demonstrated by the example of unavailabilities of safety systems.

Owing to the obligation to report all changes in availability, the monthly plant report contains a survey on the occurred unavailabilities of safety systems - see picture (4).

The period between the moment of outage and the time "ready for work" did not exceed the permissible outage time of 7 days as it is stated in the operating manual. The date "ready for work" is within the "deadline for end of outage".

By these figures on overall survey on the reliability of the safety system can be evaluated, as it is done every year by the Authorised Inspection Agency (TÜV).

2.2.2 Records of faults in the reactor protection system

The faults and defects in the reactor protection system are treated in detail - see picture (5).

Every correctly maintenance such as: replacement of measuring transducers or assemblies, or correction of drifting-appearances has to be recorded by the shift personnel in the "equipment-control log of the reactor protection system". The record is evaluated periodically by the utility and an independent expert regarding common mode or systematical failures. Besides, the licensing authority receives a copy of the log every month.

2.2.3 Records of changes in the safety interlock system

Specially chosen armatures of the safety system are locked in their safety-related positions to prevent malfunctions arising from operating errors. Keys of the safety system are kept in key boards, which can be opened only with the permission of the shift supervisor.
For reasons of safety one key only is allowed to be taken from one reducency at a time. The keys in the board are so positioned that a potential misuse can easily be recognized.

The shift supervisor has to record the use of keys by date, time, name and reason for use.

This administrative procedure is part of the safety management and therefore meets the requirements on the availability of the safety system. It is supported and accompanied by the work authorization procedure in case of maintenance work.

2.3 Certificates

In a 4-month-period, after the end of refuelling outage, the utility has to prove to the licensing authority that the plant built corresponds to the plant licenced. This brings the burnup cycle to a formal close.

This evidence is given by a number of records and certificates, which cover all aspects of plantlife over a complete burnup cycle - see picture (4).

At the end of a burnup and refuelling cycle a lot of modifications and maintenance have been carried out. The scope of these works ranges from changes in the safety system, which are of safety-related significance, or insertion of modified fuel elements down to the replacement of a valve spindle or a pump.

The utility makes a "report on construction and pressure test" for each system (6 in all), which covers the whole scope of works done in the system, regardless of their significance for safety.

On this basis a "certificate of construction and pressure test" for each system is made by an independent expert testifying the admissibility of these measures.

The proper working of the plant equipment during the burnup cycle and the refuelling period has been surveyed by in-service tests. Each test carried out in the presence of an independent expert is certified to the utility, which makes a total of 950 "certificates of in-service tests" at the end of the refuelling period.

The results of these tests together with further findings of inspections of operational data and records are documented by the independent expert in 120 "certificates about inspections of operational data and records".

The procedure ends in a renewal of the 122 "certificates of acceptance and operational test", which - in a retrospective view per annum - prove that the working and construction of all systems are within the confines of the operating license. These documents are executed by independent experts as well.

The above described procedure of reference about the licensed state of the plant is - in our view - partly redundant, regarding the control and paperwork done by the utility and the independent expert. It reflects and characterizes, however, the current situation of the licensing and supervising procedure under the German Atomic Energy Act.

2.4 Procedure of documentation

Documentation is the systematical compilation of those records necessary to or important for giving proof.

The documentation aims at
- describing the actual state of equipment
- describing the designed or specified state of equipment
- enabling a comparison between actual and designed state
- making an evaluation possible
- giving informations of surveillance tests carried out and its results.
The permanent files are divided into different sections: see picture (7).

- **Section A**: Licensing-related documents
  - 220 file folders

- **Section B**: Quality-related documents
  - 3200 file folders

- **Section C**: Documents of operation procedures
  - 1600 file folders

- **Section D**: Original drawings
  - 35000 pieces

- **Section E**: Commercial documents
  - 210 file folders

A computer-controlled documentation system keeps the records.

Review and approval procedures are in use to safeguard a proper revision and update of documents such as safety analysis reports, technical specifications, operating procedures or checklists. A document control performed by the quality control group prevents the use of outdated or not yet authorized documents or drawings.

3. Application for modification

In view of reliability assurance some aspects are of major importance, when it comes to carrying out modifications in a nuclear power plant. These are:

- classification of the modification related to their significance for safety

- consideration of all documents related with the modification

... 10

. taking into account safety standards

. consideration of tests

. approval, review and release functions

To fulfill these requirements a formal procedure has been established, which differs according to the degree of approval demanded - see picture (8). The cover sheet of the application form contains the above mentioned points.

Those responsible for modification have to classify it by its safety significance (category of safety significance). These are the categories:

- **essential modifications**

  Modifications of **direct** safety significance have to pass through a licensing procedure, such as essential modifications in the safety system affecting design.

- **non essential modifications**

  **Category 1**

  Modifications of **minor** safety significance such as insertion of slightly different fuel elements or changing of the physical limit-value in the safety system like a trip level of the core cooling system.
A formal consent of the licensing authority is based on an evaluation of an independent expert and is necessary to start work.

- **Category 2**
  Modifications of this category are without safety significance, but involve changes in the documents of the licensing procedure such as modifications of trip level in systems without safety significance.

The licensing authority confirms that the modification is classified rightly and then work is allowed to start.

- **Category 3**
  This category contains modifications without safety significance and no changes in documents of the licensing procedure are involved such as improvements in a minor logic module (adjusting a time relay).

A permission of the plant-management only is necessary to start work.

All documents which have to be revised, are listed on single pages and have to be named with a review index.

Information on necessary tests are listed on a supplementary page. Constructional tests like material verification, surface crack test or leakage rate test, have to be distinguished from those carried out for operational reasons.

An internal approval, review and release procedure has been developed which safeguards an independent quality control considering formal aspects. Besides, the correctness of classification is checked by the department of quality assurance. The department provides for the final release by the signature of plant management.

In 1985 a total number of 109 applications - two of them essential applications, 26 of category 1 and 163 of category 2 and 3 - have been released.

4. **Report on maintenance**

Appropriate maintenance is essential for a permanent safe and reliable operation of a nuclear power plant. The range of activities of the maintenance programme includes service, overhaul, repair, replacement of parts and, as appropriate, testing, calibration and inspection.

As far as interests of reliability assurance are concerned a monitoring system has been established to supervise safety- and safety-related systems at the level of safety which is required to perform the intended function throughout plantlife.

For this purpose the following aspects have to be considered.

- classification of maintenance related to safety significance
- establishment of a method of distinguishing which systems and type of equipment have been subject to maintenance
- consideration of tests to prove correct restoration
- quality control of maintenance-related documentation

Therefore a procedure of "Report on maintenance" has been established - see picture (9), which enables the utility and the independent expert to observe mode and rate of failures and the development of system reliability.

How many different kinds of maintenance work have been carried out in equal systems or on equal components can be evaluated by means of an identification number together with the alpha-numerical character.

The classification reflects the relations between

- the safety-related significance of each system and
- the modes of maintenance
The systems are classified in

- safety systems and/or components
- safety-related systems and/or components
- systems and/or components of high energy content
- systems and/or components of high activity content
- lifting equipment under nuclear standards.

The modes of maintenance are graded in

- replacement with welding at the pressure retaining boundary
- replacement necessary because of an approaching or already occurred malfunction
- preventive maintenance
- Repairs
  - with structural influence on the pressure retaining boundary (e.g. by welding)
  - without structural influence

A matrix, which combines these criteria determines on the classification. This is similar to the three categories which are "consent, approval, permission."

Safety-related and non-safety-related equipment is distinguished in respect of design and quality assurance requirements. Therefore great attention has to be paid to the maintenance-related documentation. The utility certifies the correct updating of the quality records (field No. 9, picture (9)).

The back page of the report - see picture (10) has to be completed with detailed informations about necessary test procedures for proving the restoration of the correct operable state and the documentation of test.

On the long run the reports on maintenance constitute a collection of data, which contribute to a more reliable evaluation of the failure frequency of systems or components.

5. Work authorization procedure

The work authorization procedure is an instrument of plant management

- to establish safe working conditions concerning radiation, pressure, temperature and industrial safety
- to safeguard the proper removal of systems from service
- to restore systems to correct operable state
- to check the correct performance of work by tests.

The non-observance of any of those aspects may cause danger for the working personnel, endangers the availability of systems when taken into service or risks the reliability of systems on the long run.

Therefore the procedure in use divides into

- the "work authorization" to bring the system into the appropriate state before and after work
- the "work permit" to establish safe working conditions at the working place.

To safeguard that all safety aspects have been met by the given standards a detailed check and re-check procedure is in operation.

The release of the documents depends on the final signitures of the senior responsible, of a representative of the radiation protection and of the plant management.

The release "ready for work" follows from the approval of the shift supervisor.
5.1 Prescribed Form Sheet: Work Authorization

The work authorization form sheet is in particular an instrument of the shift supervisor and contains only general information about the system, kind of work and the necessary precautions of industrial safety - see picture (11).

Instead, details are given about plant or system conditions and on systems' removing from and bringing into service. These include information about integral tests to verify the correct operable state.

The permissible maintenance time has to be mentioned explicitly, if safety- or safety-related systems are affected. This information refers to the requirements of the plant operation manual. In case of a necessary pressure relief a person has to be named responsible for carrying out and checking the pressurelessness before starting work.

A revision of the test by an independent person is necessary after works have been carried out in safety systems. This re-check is ordered by the plant management.

At the bottom of the sheet the necessary "work permits" characterized by the job number are listed.

The release for restoration will only be given when all "work permits" have been signed as carried out and are physically present at the reactor control room.

5.2 Prescribed Form Sheet: Work Permit

This sheet contains particular details to establish safe working conditions e.g. in the field of radiation protection or industrial safety.

If steps in the progress of work are important to plant operation, such as the opening of a valve with a supposed activity release, they have to be reported to the shift supervisor (notification order to shift supervisor).

The work permit is time-limited. Its validity has to be renewed after expiration.

At the bottom of the sheet routine tests suitable for checking the correct completion of work are listed.

If the work is related to a modification or a maintenance, it has to be declared in the corresponding fields on top of the form.

6. Display of Core Cooling Systems

In case of abnormal occurrences or under accident condition satisfying informations are of great importance.

- about the status of the core with the associated cooling systems and
- about the status of the containment including the containment pressure boundary isolation valves.

The "display of the core cooling systems" gives the necessary informations.
It is part of the main panel in the reactor control room and shows the reactor pressure vessel, the containment and all instruments, which are necessary for the evaluation of accident conditions, such as:

- Pressure of the reactor pressure vessel
  measuring range: 0 - 250 bar

- Level in the reactor pressure vessel
  measuring range: 0.5 m - 9 m
  9 m - 22 m

- Temperature in the pressure suppression chamber
  measuring range: 20 °C - 120 °C

The wide measuring range was introduced in the aftermath of the TMI-accident to rule out wrong evaluations due to narrow measuring ranges.

The systems shown are delineated as flow charts showing the essential pumps, valves and pipes. The vertical arrangement of the components has been considered in the chart. A component in operation is characterised with a green sign while those being out of service are red. These signals are led away immediately from components they are related to.

Apart from its above mentioned designation in case of emergency, the display gives a overall information during normal operation as well.

7. Quality assurance

According to the requirements of the German Nuclear Standard KTA 1001 "General Requirements to Quality Assurance" the utility has established quality assurance functions - see picture (13).

The department "Quality Assurance and Licensing Procedure" is responsible for the establishment and execution of the quality assurance programme. It is subordinated to the technical management and, regarding to management level, equal in status to the other departments. It is, however, independent on any direct responsibility for performance of the activities subject to quality assurance.

A quality assurance programme is partly established and complies with the requirements of the nuclear standard. It is documented by written policies, procedures and/or instructions.

To receive written instructions interviewing led to factfindings, a process which started at the end of 1984 and has just been completed. In this phase all persons of the nuclear power plant performing activities which affected safety-related functions have been questioned. It is not surprising that these interviews sometimes discovered unrecognized quality objectives in the performing functions.

Furthermore it has soon become clear that in the first time of introduction the adequacy of the instructions has to be reviewed frequently. Until now quality problems have been identified by checking or inspection. Especially the issue of documents including changes thereto and the procedures of testing have been controlled. But, formal internal audits have not been carried out until now, mainly because of the lack of adequate written instructions.
### Quality characteristics, assumptions, requirements

<table>
<thead>
<tr>
<th>Manufacturer/contractor</th>
<th>Independent experts</th>
<th>Licensing authority</th>
<th>Utility</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Redundant design</td>
<td>- Reliability data</td>
<td>- Operating staff training</td>
<td></td>
</tr>
<tr>
<td>- Specifications of</td>
<td>- Frequency of testing</td>
<td>- Safety and operation-related reports</td>
<td></td>
</tr>
<tr>
<td>e systems</td>
<td>- Scope of surveillance tests</td>
<td>- Procedures of documentation</td>
<td></td>
</tr>
<tr>
<td>e components</td>
<td>- Maximum autogague</td>
<td>- Quality assurance programme</td>
<td></td>
</tr>
<tr>
<td>e material properties</td>
<td>- Fitting position of</td>
<td>- Industrial safety provisions</td>
<td></td>
</tr>
<tr>
<td>e testing of materials</td>
<td>selected valves</td>
<td>- Maintenance programme</td>
<td></td>
</tr>
<tr>
<td>- Industrial safety provisions</td>
<td></td>
<td>- a preventive maintenance</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Modification programme</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Work authorization procedure</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Procedures of providing material</td>
<td></td>
</tr>
</tbody>
</table>

**Utility responsibilities to meet safety and reliability aspects**

- Training and retraining programme
- Work authorization procedure (removal of systems from service, restoration to correct operable state, temporary modifications)
- Surveillance programme (follow up of equipment deterioration, programme for evaluation and feedback of operating experience)
- Maintenance programme (preventive maintenance, maintenance-related documentation)
- Plant modification programme (safety significance)
- Procedure to procure, receive, store and issue spare parts relevant to safety
- Procedure of documentation and reporting
- Review and approval process, document control
- Quality control – Quality assurance (quality control separated from quality assurance function)

**Abb. 1**
Utility responsibilities to meet safety and reliability aspects

---

**The quality control is organized both in the departments of mechanical and electrical engineering - see picture (13). These groups have responsibilities for:**

- the control of procurement documents regarding safety-related components
- for the control of purchased materials and equipment (e.g., welding) are in accordance with applicable standards or specifications
- for the control of purchased material and equipment
- for the identification and control of safety-related material or equipment.

**The demonstrated organizational structure of two independent quality functions is, in our view, the best method to meet arising quality problems.**

<table>
<thead>
<tr>
<th>System</th>
<th>Grund für Nichtverfügbarkeit</th>
<th>Datum/Uhrzeit</th>
<th>Spätertermin für Wiederverfügbarkeit</th>
<th>Betriebsbereit Datum/Uhrzeit</th>
</tr>
</thead>
<tbody>
<tr>
<td>VE41</td>
<td>Austausch der Rückschlagklappe</td>
<td>12.12.84 03.30 Uhr</td>
<td>19.12.84 03.30 Uhr</td>
<td>12.12.84 19.00 Uhr</td>
</tr>
<tr>
<td></td>
<td>VE41 3102</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Replacement of nonreturn flap</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TH45</td>
<td>Freischaltung *</td>
<td>12.12.84 03.30 Uhr</td>
<td>18.12.84 03.30 Uhr</td>
<td>12.12.84 19.00 Uhr</td>
</tr>
<tr>
<td>VG41</td>
<td>Nebenkühlwasser VE41</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE31</td>
<td>Freischaltung *</td>
<td>12.12.84 03.30 Uhr</td>
<td>18.12.84 03.30 Uhr</td>
<td>12.12.84 19.00 Uhr</td>
</tr>
<tr>
<td>FY23</td>
<td>Nebenkühlwasser VE41</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Freischaltung *</td>
<td>12.12.84 03.30 Uhr</td>
<td>26.12.84 03.30 Uhr</td>
<td>12.12.84 19.00 Uhr</td>
</tr>
<tr>
<td>TJ</td>
<td>Nebenkühlwasser VE41</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Freischaltung *</td>
<td>12.12.84 03.30 Uhr</td>
<td>08.01.85 03.30 Uhr</td>
<td>12.12.84 19.00 Uhr</td>
</tr>
</tbody>
</table>

*) Removal of systems from service in consequence of repair work VE41

VE Service water system
TH Low pressure coolant injection system & decay heat removal system
VG Closed cooling water circuit
TZ Containment loop recirculation system
FY Diesel generator (emergency power unit)
TJ High pressure coolant injection system

Abb. 4 Monthly plant report: Unavailabilities of safety systems
Procedure of reference about the status of the plant

Archiv

Section A
- Licensing-related documents
  220 file folders
  - License applications
  - Conditions fulfilled
  - Partial construction permits
  - Safety analysis report
  - Operating license

Section B
- Quality-related records
  3,200 file folders
  - Rules/regulations specifications
  - Records of preexamination
  - Certificates of tests
  - Records of spare parts

Section C
- Records of operating procedures
  1,600 file folders
  - Data
  - Plant operating manual
  - Records relevant operation e.g.
    - flow charts
  - Maintenance related records
  - Preoperational program/tests
  - Technical reports
  - Life duration records

Section D
- Original drawings
  35,000 pages
  - Drawings e actual state
  - Drawings e history

Section E
- Commercial records
  210 file folders
  - Correspondence
  - Offer
  - Purchasing orders

Structure of documentation
Table: KKK durchzuführende Prüfungen

<table>
<thead>
<tr>
<th>Terms to be carried out</th>
<th>KKK</th>
<th>durchzuführende Prüfungen</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard tests</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control of direction of rotation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control of starting torque</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Leakage test</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Construction and pressure test</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Record</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acceptance and operational test</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Record</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sonstige Prüfungen</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Abb. 10
Prescribed form: Report on maintenance (side)

Diagram: Work authorization

Abb. 11
Prescribed form: Work authorization
An extensive probabilistic study of the safety-related systems was performed for the Alto Lazio Nuclear Power Plant, located in Italy. The analysis, conducted by a team consisting of engineers from ENEL (utility), General Electric (US nuclear equipment manufacturer), and Ansaldo (plant architect engineer), was performed on a two-unit BWR/6 plant, which was recently brought into operation. Extensive calculations were performed on the design of the system, performance of special accidental analyses of the issuing documents were reviewed and verification of the design engineers over 250 man-months, with a total effort of more than one hundred engineers. Although the RAPP (Safety and Reliability) database was developed, there are several differences when compared to the original ATRB database. The final report also included a detailed presentation of the preliminary analysis results, with the emphasis being placed on the frequency of events in the licensing process and the need for ongoing plant operation.
control function. Licensing models were used to find the minimum number of necessary mitigating systems, instead of the "best estimate models" used in other PRA studies.

2.2. Analysis Purposes

The purposes of the ALSRA study were:
- to ensure the ENEA requirement of the Alto Lazio Construction Permit for a reliability analysis of the safety systems;
- to provide a plant reliability model to obtain more rational and unique Technical Specifications for Alto Lazio;
- to identify critical areas in design which need correction or improvement from the safety or plant availability point of view;
- to make decision on proposed design modifications and to choose the optimal solution among alternatives;
- to support the resolution of licensing issues or of problems which might occur during the nuclear test and power operation;
- to provide a better understanding of the integrated response of the plant to transients and accidents, even in the event of multiple failures.

2.3. Methodology

As first step of the analysis, comprehensive Failure Modes and Effect Analyses (FMEA) were performed for all safety systems and for additional systems important to the plant availability. The FMEA task consumed about 60% of the total effort of the ALSRA team, but was a very valuable task. It provided detailed knowledge of the system, the basis for the construction of the system fault tree, the single failure criteria verification at the system level, and the review of the design from the point of view of the surveillance test feasibility.

In addition, the FMEAs will be the basis for the operating personnel to decide whether the system is to be declared inoperable, following the failure of a particular component, and the basis for the construction of a trouble shooting chart.

Following the FMEA task and the thermohydraulic analysis to determine the minimum configuration of the core cooling system, the tasks performed were the development of the event scenarios and of the interdependence matrices, the fault tree construction, the functional fault tree analysis by the SETS/SEP computer codes and the event tree analysis. The performance of the FMEA was possible due to the optimal ALSRA timing.

The design was close to being completed and frozen so that a precise and detailed analysis was possible, and the plant construction status was such that it was still possible to correct the discrepancies and to incorporate significant reliability improvements without any plant construction delay.

2.4. Results

The analysis was conclude in 1984 with the publication of 23 reports, containing the details of both qualitative and quantitative analysis.

As a consequence of the analysis many design change recommendations were implemented to improve the plant safety and availability or to correct design inconsistencies.

The most significant design changes were made on the control building and control room ventilating systems. The preliminary analysis found that the failure of one of the above systems during normal operation was the major contributor to the plant risk of exceeding the licensing criteria for the core cooling and containment cooling functions. The proposed design change modifications were based on the reliability models which allowed a quick decision on their implementation. The prompt response minimized the construction delay and cost.

The quantitative analysis results for the frequency of exceeding the accident licensing criteria for the core cooling are contained in Tab. 1. These results show that Alto Lazio has an excellent reliability of the network of the mitigating systems and of their auxiliaries to respond to the transients and accidents events. This result is more significant in that it was obtained by performing a conservative reliability analysis using the licensing criteria.

3. PUN-PWR PROBABILISTIC SAFETY STUDY

3.1. Introduction

The Italian Energy Plan called for the construction of 10,000 MWe (nuclear) within the next decade. An important point of this plan is the adoption of a standard design for the nuclear unit - Progetto Unificato Nucaleare (PUN), to be applied to a standard station of 2 PWR Units, 1000 MWe each.

The PUN design consists of a standard Westinghouse three-loop nuclear supply system.
A further requirement of the energy plan is that a detailed safety evaluation be performed on the preliminarily approved conceptual PUN design and be used to evaluate the safety criteria for the future nuclear plants. Therefore, in December 1982, ENEL decided to perform a level 1 Probabilistic Risk Assessment on the preliminarily approved PUN design. The primary goal of the safety of the PUN design was attained by means of an assessment of the core damage frequency, the second goal was to identify the system weak points. Furthermore, ENEL decided to maintain the study as a continual living document to be used as a tool to assess in terms of risk-effect any additional regulatory requirements that might be required during construction and operation life of the plant. Three organizations, ANSALDO, ENEL and Westinghouse assisted in performing the probabilistic safety study, with Westinghouse providing the technical lead and technology transfer.

The experience gained in performing the study revealed that through careful application of the probabilistic technique, the study can be used as a tool to develop an optimum plant design in terms of safety and cost.

3.2. Probabilistic Safety Assessment (PSA) Design Evaluation Process

After developing the conceptual design, the intent of the PSA design evaluation process was directed towards the identification of potential improvements to the conceptual design which would significantly improve public safety. These design improvements can be implemented into the conceptual design before beginning of construction, thus reducing plant modifications costs. Then, alternative design options can be evaluated using probabilistic techniques, and a simplified design can be implemented to reduce capital cost without sacrificing public health and safety. The overall use of the PUN-PSA, starts with the development of the conceptual design based on traditional deterministic safety criteria. The conceptual design can then be evaluated using probabilistic risk assessment techniques to produce a baseline risk.

After quantification of the core damage frequency (CDF), engineering recommendations on the design were proposed to achieve the best value of CDF. These recommendations stemmed from the sensitivity studies carried out previously. At the conclusion of the individual sensitivity study, those factors in the plant design configuration having the strongest impact were combined to determine the overall impact on core damage frequency.

3.3. A living Probabilistic Safety Study

The PSS model and methodology had to be flexible to accommodate design changes and to be automated to the maximum possible extent to minimize the manpower required to analyze potential design changes. To meet this requirement, the PSS became an automated living tool which could be quickly updated with little effort. The process associated with using a living PSS model is shown in Figure 1. The living PSS model will be used to evaluate design changes and operating procedures implemented during the construction, testing and operational phases of the plant. In addition, the PSS model will be used to evaluate regulatory requirements that may be imposed during the life of the plant.

With this in mind, the PSS was developed on a modular basis in which each module represents a particular individualized analysis such as initiating events, system fault tree models, event tree models and support state model. These modules were then analyzed and combined using integrated PRA computer codes which enable the risk assessment engineers to evaluate any changes using automated techniques. Having the entire model computerized and readily available for re-analysis helps in fulfilling the living PSS requirement.

3.4. Results

The first phase of PSS was concluded in July 84 and the mean value of Core Damage Frequency (CDF) was calculated to be 4.4. E-05/year for internal events and loss of offsite power.

The outcomes from the study were generally favourable for the design, showing a good balance of plant systems; no single accident sequence accounted for more than 10% of the total CDF. In all, over 70 significantly contributing accident sequences were identified. However this final result did not yet comply with the ENEA criteria on CDF (≤ 1.0 E-05/y) and, therefore, some engineering recommendations were proposed. Since no single system modification could decrease the CDF significantly, ENEL decided to study a set of reasonable design changes. The basic criteria was that any proposal would not deviate from the proven and mature PWR technology. Taking into account also the relevant conservatism included in the PSS methodology and hypothesis, and the advantages that could be
gained from more sophisticated studies, any design modification impacting the CDF for less than 5% was been considered negligible.

A series of sensitivity analysis were performed in order to identify pertinent investigation areas; they covered the PSS model operator's actions, initiating event frequencies and possible alternate design configurations. Fifteen alternate design configurations were examined on the basis of one design modification at a time, and then evaluating the contribution of each modification as a percent reduction in CDF of the PSS base case. Some modifications were aggregated when related to the same system and so their final number was reduced to six. They are related to the following systems:
- Safety Injection
- Residual Heat Removal
- Service water and Component Cooling
- Vital ac/dc electrical
- Back-up protection
- Logic of reactor trip.

The above list includes the modifications in decreasing order of importance related to their impact on reducing the CDF (fig.2-3).

On the basis of all the preceding modifications a new combined sensitivity for the PSS was calculated, and the result showed a reduction in CDF to 8.0 E-06/year.

The study was reviewed by the Safety Authority and the engineering recommendations are being implemented.

3. LATINA-MAGNOX PROBABILISTIC SAFETY STUDY

3.1. Introduction

Just after TMI accident, the Italian Safety Authority ENEA requested ENEL to perform a complete reevaluation of Latina of Latina plant safety, on the basis updated standards and criteria, in order to demonstrate the possibility to maintain the plant in operation for a further long period.

The study was completed in four years and enabled ENEL to single out many plant modifications to be performed, on a deterministic basis, in order to meet the criteria taken as references.

In 1985, ENEA requested an evaluation, thorough a probabilistic study, of the level of safety reached by Latina plant, modified according to the results of the aforesaid analysis.

Another use of this study should be the possibility of giving the right priority to the corrective measures now in the implementation phase, and to check their validity with an independent method.

The study should be completed by the end of 1986 and, also on the basis of its results, a decision will be taken about the plant future operation schedule to continue that, to date, is till 1992, i.e. 30 years after the first commissioning. The work is performed by the NNC (National Nuclear Corp.) and ENEL, involving operational personnel from the plant.

The assessment will deal with the identification and quantification of the frequencies of initiating events and fault sequences which might lead to core damage.

It is intended that the assessment forms a basis for an initial evaluation of the safety status of the existing plant, together with certain planned modifications already defined by other studies, and it is going to be performed at an appropriate level of detail. It is recognised that the study should be capable of extension in scope and detail into a more comprehensive risk assessment.

The study is being developed according to the follow criteria and hypotheses:
- Internal events and/or initiating events related to the electrical grid that could lead to degraded core conditions will be considered.
- Plant behavior will be analyzed to determine and to verify the integrity of the fuel in the core during and following the accident scenario defined through event trees.
- Best estimate data, evaluation models and acceptance criteria will be used; where information is lacking for specific components, adequate conservatism will be introduced in the reliability evaluations and a sensitivity analysis will be performed if necessary.
- Sensitivity analysis will be performed for those dominant event sequences, for which uncertainty factors might, be more important than in other sequences.
- Human reliability will be considered according to a probabilistic methodology, without deterministic constraints on operator availability.
- Common cause failures will be carefully addressed.
- Recovery will be considered for electrical supply systems (external grid and diesel generators), and where specific components are critical for system availability, the possibility of their recovery will be examined.
- All the assumptions, data, functional operation, system and procedure models will reflect the Latina NPP, as much as possible, with the improvements to existing equipment and to the operational and maintenance procedure already defined.
3.2. Methodology

The characteristic of gas cooled reactors is such that, following most faults, the potential event sequences are very similar after the reactor is shutdown, and successful cooling can be achieved provided a minimum of protective equipment operates. For this reason, based on experience of similar assessments, the method of small event trees-large fault trees was preferred, also because considered particularly appropriate for the decay heat removal systems.

4. CONCLUSION

The experience gained from the three studies provided the following insights:
- Early application of PSA techniques to identify weak points of the design allows for inexpensive system modifications (no dramatic changes are needed) that not only reduce core damage frequency, but can be also used to reduce the frequency of serious releases.
- A major side benefit of evaluating the design has been the integration of the design and safety engineering teams.
- Application of PSA techniques to the total plant design allows the risk effectiveness determinations to be considered as part of the final decision.
- Ability to enhance the understanding of accident sequences, components, and systems so that appropriate attention can be paid to these areas during design, construction, training, and operation.
- The evaluation of the safety level of operating plants through PSA allows identification by the utility of the weak aspects (operators, maintenance, test etc.) specially during operation of the decay heat removal systems.

The PSA tool should be the useful way to understand the level of safety of a NPP: however, trying to directly transfer the numerical results of a probabilistic assessment from one plant to another could jeopardize the credibility of the tool. Every nuclear power plant has its own frequency of core damage and of serious releases that depends on the peculiar aspects of the station under examination, provided the completeness of the analysis and the methodology used are followed on the same basis.

### TABLE 1
FREQUENCY OF EXCEEDING LICENSING ACCEPTANCE CRITERIA FOR CORE COOLING IN THE ALTO LAZIO NUCLEAR PLANT

<table>
<thead>
<tr>
<th>Initiators</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOOPS EVENTS</td>
<td>2.16E-6</td>
<td>36.9</td>
</tr>
<tr>
<td>OTHER TRANSIENTS (mainly loss of feedwater and isolation events)</td>
<td>1.77E-6</td>
<td>30.3</td>
</tr>
<tr>
<td>LARGE LOCA: Inside Drywell</td>
<td>5.9E-7</td>
<td>10.1</td>
</tr>
<tr>
<td>CONTROL BUILDING HVAC LOSS</td>
<td>4.8E-7</td>
<td>8.2</td>
</tr>
<tr>
<td>INTERMEDIATE LOCA-Inside Drywell</td>
<td>4.6E-7</td>
<td>7.9</td>
</tr>
<tr>
<td>ECCS LOCA-Inside Drywell</td>
<td>2.5E-7</td>
<td>4.3</td>
</tr>
<tr>
<td>CONTROL ROOM HVAC LOSS</td>
<td>1.1E-7</td>
<td>1.9</td>
</tr>
<tr>
<td>SMALL LOCA-Inside Drywell</td>
<td>1.3E-8</td>
<td>0.2</td>
</tr>
<tr>
<td>OTHER LOCA</td>
<td>9.3E-9</td>
<td>0.2</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td>5.8E-6</td>
<td>100.0</td>
</tr>
</tbody>
</table>

LOOPS = Loss Of Off-site Power  
LOCA = Loss Of Coolant Accident  
HVAC = Heating Ventilating, and Air Conditioning
FIG. 1

FIG. 2 Phase 1 - Sensitivity Results
FIG. 3 REDUCTION ON CORE DAMAGE FREQUENCY DUE TO SYSTEM MODIFICATIONS
This paper discusses the application, now in progress in Italy, of the PSA for the Italian Standard Project which makes use of numerical targets, as far as the probability of core melt accidents is concerned.

This application was conceived for providing the Regulatory Body with an additional tool for making decisions in high uncertainties areas, an so for developing mandatory requirements related to specific plant provisions or design changes having safety implications. The purpose was to assess the maximum effort to be made in view of achieving the highest safety levels in the plant design and operation on the light of the most updated and well proven technology.

The paper describes the PUN/PSA specifications which were required by the Regulatory Body in order to achieve the wanted objectives. The methodology for the analysis is similar to that used for other level 1 PSA.

The staff of the Italian Regulatory Body reviewed the PSA in order to assess the adequacy of the study with the existing status of the art and to verify compliance with the required specifications.

The staff recognized the high technical quality of the study and concluded that it may be used as a tool for judging the safety level of the PUN design, being this level expressed by the assessed probability value of core melt accidents. However since results of the first issue of the PUN/PSA have shown that the assessed probability of core melt accidents is greater than the upper bound indicated by the targets, the staff made also independent analyses addressed to identifying possible design improvements or alternatives having impact on the plant safety. Results of these analyses proved that specific design changes or operation procedures are capable to reduce the probability of core melt accidents below the upper bound and toward the lower bound of the targets, as requested by the specifications for the PSA.

The paper discusses also a possible set of actions which should be of concern for future revisions and updating of the PSA, when the PUN design development and licensing process will allow to make more realistic acceptable assumptions on the plant features and operation. Finally it points out that this study needs to interact continuously with the PUN design development, and with construction and the
operation of specific plant units as well. The PUN/PSA could therefore be used as a living schedule for judging the plant safety level and for making safety decisions in any moment during the life of the plant itself.

1) Probabilistic targets for core melt accidents

The use of probabilistic techniques has been recently introduced in the Italian regulatory process. The last application has regarded the Italian PWR Standard Project (PUN), for which the Italian Regulatory Body requested to make a PSA with the use of numerical targets as far as the probability of core melt accidents is concerned. The purpose was to provide an additional tool for making decisions in high uncertainties areas, being the decisions aimed at indicating specific plant provisions or design changes having safety implications. Therefore, in view of this advanced use, the PUN/PSA was planned and implemented with the following three objectives:
- to make a systematic assessment of the plant behavior under accident conditions caused by specific initiating events;
- to make a balance assessment of the plant defences which are called to face accident sequences leading to exceed core cooling limit conditions (core damage);
- to provide support to practical improvements that could be cycled back into the design.

It was requested that the overall probability of exceeding the core coolability limits had to be in the range $10^{-6}$ and $10^{-5}$, and that design improvements had to be adopted in order to push the probability towards the lower bound. In any case $10^{-5}$ was the upper bound not to be exceeded.

The methodology used for PUN/PSSS was similar to that described as level 1 PRA in NUREG/CR-2300 "PRA Procedure Guide". It implied a
preliminary acquirement and understanding of the plant information, the identification and grouping of initiating events, the development of event scenarios and event frequency data base from existing data and plant design specifications. Success criteria were developed from transient and ECCS analyses using, as much as possible, realistic models and plant performance parameters.

Operator errors in procedures implementation, system dependencies and common cause failures were also taken in due account. The analysis considered only internal events, whereas external hazards, both natural and man made, were excluded. Sensitivity analyses were also performed in order to assess the influence on probability estimates of specific plant parameters and of engineering assumptions used in modeling the plant response and system behaviours.

2) The review of PUN/PSA by the regulatory staff

The PUN/PSA was submitted for approval to the Italian Regulatory Body. The plant design and the safety analysis were examined by the review staff in order to verify their compliance with the probabilistic targets as required by the specifications. This task firstly implied that the submitted application received assurance of high technical quality. Therefore the staff made a review aimed at determining whether the methodology used in the study were consistent with the current status of the art, assessing the correctness of the applications themselves in specific key areas, and identifying strenghts or weaknesses of the study in specific technical areas which are matter of concerns for most other studies.

Special issues were put forward that are specific of the methodology used in the study and/or affected by the requirements involved in decision making. The first issue was the case of methodology used in the Support States analysis which separates Support Systems from Front Line Systems. This methodology requires careful reading to discover if the separation makes some aspects lost (for instance at the system interface); in fact it is less straightforward than others which merge all Front-Line and Support Systems in each core damage sequence.

Another issue was to recognize diversity in safety actions. The analysis aimed at identifying potential common factors (like type of power source, layout, maintenance) and decisions were made on objective factors supported, if necessary, by judgment.

The main issue, however, was the extent of upgrading of plant design which is required in the light of analysis results.

It must be mentioned that the decisions made on the results of probabilistic studies must be considered always in the frame of a deterministic process. Namely the probabilistic requirements used in the application are to be regarded as reference numbers to be accounted for when making decisions. The requirements are aimed at determining whether the maximum effort is made with a view to achieving the highest safety levels in the design development. These levels correspond to the lowest probability values that can be achieved through the adoption in the design of technological
choices which make use of well proven components and methodologies.

For these considerations the review was also addressed to identifying potential design and/or procedure alternatives to meet the above mentioned lowest probability values. To this purpose a specific methodology was used by the review staff. The methodology gives emphasis on assessment of functions required to prevent core melt and on the adequacy of the design. The identification of design/procedure changes was supported, to the maximum possible extent, by available information, and includes sensitivity and importance analyses using overall accident frequency information.

The analyses included the evaluation of the importance of the main factors such as system operation, human actions and consequential events, with respect to core melt frequency.

3) Indications given by the review

After the PUN/PSD review the staff recognized the methodology overall adequacy and concluded that the study can be used as a tool for judging the safety level of the PUN design. This is expressed by the assessed probability value of core melt accidents.

However it was stated that the PUN/PSD was planned and implemented at a stage of the project development that much information was not yet available (for instance the design of particular systems, operational and emergency procedures, specific accident and transients analysis, detailed design of systems and their lay-out).

For the above reasons both conservative hypotheses and work assumptions were needed for carrying out the PUN/PSD. They were based either on information from generic studies and other PSA, or on best estimates and engineering judgments (this was the case, for instance, for estimating the frequency of the SGTR event or the unavailability of the IPS).

The review staff made independent analyses aimed at investigating the sensitivity of the core melt probability to more pessimistic but still acceptable hypotheses. The analyses pointed out the need that the PUN/PSD should be continuously revised and updated during the future design developments. In fact through these analyses it was possible to identify a set of actions which are needed for confirming the work assumptions made for the first issue of the PUN/PSD. The actions are also aimed at providing new information for future revisions and updating. Times to implement the actions depend on the subjects to be treated and on the schedule envisaged for the design developments and approvals.

A list of topics which are of concern for future PSA actions was proposed by the review staff (see table 1). Some of them specifically are addressed to the methodology used in the study and require to follow the design development for making future more realistic assumptions. Other actions will be needed in order to better investigate the implications of the operator behaviour when the operating and emergency procedures will be ready and presented to the Regulatory Body for approval. In any case all the actions are susceptible to be considered for defining possible
mandatory requirements which could be adopted within the frame of the PUN licensing process.

4) Probability reduction analysis for core melt accidents

The results of the PUN/PSA first issue were not in agreement with the probabilistic targets. In fact the study assessed a core melt probability value greater than $10^{-5}$/yr, as required by the specifications. In addition this figure didn't include contribution of area events, such as plant fire.

The PUN/PSA, however, was also used for identifying and suggesting design modifications aimed at decreasing this probability value and thus at improving the plant safety level.

In the course of the PSA review the staff performed an analysis of the various plant systems in order to rank the importance of their respective safety and auxiliary functions. The analysis was used for assessing both the balance of the plant against different accident situations and the safety improvements obtained by the design modifications. In addition the importance analysis allowed to identify weakness areas for further possible improvements (e.g. emergency feedwater and hydraulic auxiliary systems). The staff performed calculations of the core melt probability reduction due to the modifications.

Results of the staff analyses confirmed that the proposed modifications are capable to reduce the core melt probability towards the lowest values given in the specifications. The analyses, however, suggested also an additional list of topics to be considered for the development of the design modification and for future PSA revisions and updating (see table 2). Since uncertainties still persist in the assessed values further actions have been therefore envisaged in order to remove over estimations on the core melt probability due to the work assumptions made for the calculations.

5) Conclusions

Due to the incompleteness of the design development, and the lack of information on operating procedures, it is not possible to conclude now that full compliance is met of the PUN design with the probabilistic targets given in the PSA specifications. However the first calculations performed after considering the adoption of the proposed design modifications showed that a value lesser than $10^{-5}$ may be obtained for the core melt accidents probability.

At present it is expected that the highest probability levels will not be exceeded when all design and operation details will be available, so that it will be possible to redraft a final and updated version issue of the PUN/PSA including also the area event analysis.

When demonstration will be given that the probabilistic target are fully met, the PUN/PSA will be capable to support the Regulatory Body decisions for developing the design regulatory guides, the operating technical specifications and any other action having implication with the plant safety.

From the above considerations it may be concluded that the PUN/PSA
needs to interact continuously with the design development and with
the construction and operation of specific plant units as well. By
this way it may provide the Regulatory Body with a valuable and
updated tool for making decisions which are of concern for the
plant safety. It is in the staff opinion that it is well qualified
to be used as a living schedule for judging in any moment the
plant safety during the life of the plant itself.

TABLE 1

List of topics for future PSA actions

1) Uncertainties analysis
2) Support States Model
3) Success Criteria
4) Common Mode Failure Probability - Binomial Failure Rate Model
5) Steam Generator Tube Rupture Event
6) Consequential Events
7) Operator Actions
8) Test & Maintenance
9) Integrated Protection System
10) Emergency Feedwater System
11) Long Term Failures during the Injection Phase
12) RWST Valves Failure to close
13) Control Room and Man-machine interactions.
### TABLE 2

**Additional list of topics for future PSA actions**  
(from the CHF reduction analysis)

1. Modification of the Emergency Injection and Recirculation System  
2. Modification of the RHR in Low Pressure Recirculation Mode  
3. Modification of the Actuation Logic of the Steam Generator Relief Valves  
4. Addition of Switching in the Vital Buses Electrical Supply  
5. Addition of the Back up Protection System  
6. Modification of the Fluid Auxiliary System  
7. Frequency Reduction of Events caused by Auxiliary Systems Failures  
8. Frequency Reduction of Steam Isolation Valves Spurious Closures  
APPLICATION OF PROBABILISTIC SAFETY ASSESSMENT TO THE SAFETY DESIGN VERIFICATION OF DARLINGTON NUCLEAR GENERATING STATION

V.R. Bain
Ontario Hydro
Toronto, Canada

INTRODUCTION

This paper describes a probabilistic safety assessment study being carried out by Ontario Hydro of the Darlington nuclear generating station. The primary purpose of this study is to provide a thorough safety design verification of the Darlington station by ensuring that accident sequences leading to varying degrees of fuel damage are of appropriately low probability. The paper first briefly discusses Ontario Hydro's previous experience in this area, and then describes the manner in which the techniques of probabilistic safety assessment are being used to provide a systematic design review of the Darlington Generating Station. Some of the insights into plant design that the study has afforded are described, which led to the incorporation of a number of design changes. Because many of these design weaknesses were identified before the hardware was fully installed, their correction was timely and relatively inexpensive to implement.

THE DARLINGTON PROBABILISTIC SAFETY EVALUATION STUDY

Background

The value of Probabilistic Safety Studies in assessing the design adequacy of complex engineering systems, especially those that involve many engineering disciplines with significant interactions among the subsystems, has long been recognized in Ontario Hydro. A number of such studies have been undertaken in the past to assess the reliability of special safety systems such as the reactor shutdown (protection) systems, the emergency coolant injection systems and the containment systems. Also, as necessary, reliability studies have been carried out of systems whose failure could lead to a demand being placed on the special safety systems to operate, e.g., the reactor power regulating system. While these studies were of a fairly extensive nature and provided important insights into the design and operation of the system being analysed, they were, nevertheless, separate evaluations, independent of one another. For example, these studies did not seek to identify or account for potential dependencies between process systems and safety systems, or provide estimates of probabilities of occurrence of events that could lead to core damage.

Concurrent with these studies, there arose the need to assess the impact on reactor safety of support system failures, such as losses of service water, instrument air, etc., that, because of their multiple and varied effects on plant operation, could not be analysed using the stylized methodology developed to study events such as losses of coolant. It was recognized that the appropriate framework for analysing these events was a probabilistic one. Accordingly, for the Bruce A generating station event sequence and fault tree analyses were performed for such events by Atomic Energy of Canada Ltd (AECL). Ontario Hydro's Consultant. These resulted in the identification of areas of concern arising from such initiating events. Because these studies considered some multiple failures, with the results summarized in matrix form, they came to be called Safety Design Matrices (SDM).

The success of these limited event sequence studies led to the institution of a program of probabilistic studies on the Pickering B and Bruce B nuclear generating stations from 1978 to 1983. The scope was broadened to not only probabilistically evaluate support system failures, but also event sequences that might occur following initiating events such as losses of coolant and losses of feedwater. These studies played a role in the obtaining of operating licenses for these stations.

The experience gained in conducting various system reliability studies and the safety design matrix program set the stage for carrying out a comprehensive probabilistic safety assessment of Ontario Hydro's post Pickering B and Bruce B nuclear generating station, viz the Darlington Station. Darlington GS is a 4x380 MWe CANU station currently under construction, with the first unit scheduled to attain criticality in November 1987. A major difficulty in such assessments hitherto had been the unavailability of a practical methodology for handling the complexities of a nuclear power plant. However, many advances have taken place in the techniques of probabilistic safety assessments since the safety design matrix studies were begun. Therefore, when the program for Darlington GS was conceived, it was felt that an integrated study could be undertaken to identify and quantify the ways in which varying degrees of fuel damage and release of radioactivity to the public could occur following any one of a large number of possible initiating events. The program was called the Darlington Probabilistic Safety Evaluation Study (DPSE).

Study Organization and Scope

The nature of a probabilistic safety assessment study is such that technical expertise in a wide range of subjects is required to be pooled together. As well, the various subtasks need to be coordinated such that overall study goals are met. In the case of the DPSE study, this was achieved by ensuring that individuals working on the study were knowledgeable about both nuclear safety issues and the various plant systems. The study group worked in a common location under the guidance of a single individual to ensure adequacy of the analysis and consistent application of the methodology adopted.

The various subtasks undertaken in the DPSE study are as follows:

1. Identification of potential initiating events by a systematic review of plant design, such as by failure modes and effects analyses, and of past operating experience:
Development of event trees to identify mitigating systems, their failure modes of interest, and sequences of events in functional terms leading to different categories of fuel damage:

Development of detailed fault tree models of mitigating systems:

Development of a component failure database and a means of quantifying human error events:

Integration of event tree and fault tree models to identify failure sequences of concern:

Calculation of in-plant and ex-plant source terms;

Calculation of off-site radiological consequences.

The bulk of the effort is in the area of event tree and fault tree model development and quantification. Apart from being required to calculate the probabilities of occurrence of various sequences of events leading to fuel damage, the development of these plant failures logic models in itself provides a thorough review of system design. The methods being used to develop and solve fault trees and determine dominant accident sequences are described below.

METHODOLGY

In the DSF study, fault tree models have been developed in a fairly detailed manner such that the interdependencies between the various systems can be characterized as accurately as possible. Experience has shown that quite often, it is at the lower levels of the failure logic that subtle interactions exist, which can not only adversely affect a number of mitigating systems but also possibly lead to initiation of an event sequence. As well, a detailed development of fault tree models provides some assurance that the reliability estimates obtained from the fault tree are reasonable.

The development of fault trees for the various top events identified in the event trees begins at the highest level of system failure, with the analyst carefully analyzing process flowsheets, instrumentation and control drawings, and electrical elementary diagrams and one-line diagrams to determine how failures at the various levels in the event tree can occur. He would terminate the fault tree either as is usual, at those failures for which failure data exist, or where the failure mode is associated with another system being analyzed by a separate analyst. Each event in the fault tree is given a label, it being ensured that the same failure mode is given the same label in all those fault trees in which it appears. Where necessary, initiating events are directly included in the fault tree models to appropriately account for their impact on one or more plant systems.

The extensive fault tree modeling of the plant necessitated the development and use of computer-aids for storing, processing and plotting fault trees, as well as for integrating fault tree models so as to compute accident sequence probabilities. Some of these were developed in-house, primarily those that facilitated fault tree coding, review and reduction in size. The computation of minimal cut sets was done using the RPRA code and fault tree plotting by means of the PFD code, both of which are available on Control Data Corporation's (CDC) Cybernet network. Further details of these techniques are provided in Reference 1.

Failure rate data were derived from Ontario Hydro's component failure database, supplemented by external sources where such data were not available.

For the purpose of human reliability modeling, all human interactions with plant systems identified in the fault trees have been categorized as being either simple or complex interactions. By definition, simple interactions are those that occur in the course of routine tasks prior to an initiating event. All post-initiating event interactions and those pre-initiating events that involve, as an example, the disabling of a system are defined to be complex interactions. Models were developed to quantify both simple and complex interactions. Further details of the human reliability analysis are contained in Reference 2.

To provide adequate checking, all fault trees were reviewed by the study leader prior to being issued in report form for peer review, primarily by the would-be operating staff of the plant and the relevant design groups, who paid special attention to the assumptions on which the fault tree development was based.

As of now, all fault tree development is complete and interim reports have been written on all systems analyzed. A total of thirty such reports have been prepared. These include analyses of: front line, normally-operating process systems such as the heat transport system and auxiliaries, the feedwater, condensate and steam relief systems, the reactor power regulating system, the moderator system and the neutron shield cooling system: mitigating systems such as emergency coolant injection and recovery, containment, the two reactor shutdown systems, auxiliary feedwater, shutdown cooling, combustion turbine units for standby and emergency power, and support systems such as the various service water systems, instrument air systems and electrical power distribution systems. Particular attention was paid to control system design, with fault trees developed for the dual digital control system providing overall plant control, and the numerous programmable controllers being used in place of electromechanical relays. Integration of various subsystem models to ultimately obtain cutset lists and frequencies of occurrence of various categories of fuel damage and ex-plant release is underway.

BENEFITS

Although the final estimates of health and economic risk are not available yet, the study has already provided significant benefits by uncovering design deficiencies of varying impact and getting them corrected. Up to the present time, about eighty-five design changes have been made as a result of the DSF study. It is estimated that if these
were not corrected now only about one third would have been detected and corrected during plant commissioning, since these were of a nature that normal plant operation could not take place. Of the remaining, the deficiencies had one or more of the following implications:

(a) Could lead to an initiating event;
(b) Could affect reliability of a system required for accident mitigation;
(c) Could affect production reliability or lead to equipment damage;
(d) Could adversely affect the ability of the operator to take appropriate corrective action following an accident.

Some examples of such design deficiencies are provided below.

(a) Loss of signals from an electrical panel, for example, due to cable severance, on which are mounted controls for the operator to switch over to an emergency power source could lead to a loss of control power that would result in the opening of relief valves on the heat transport system, failure to automatically isolate the piping downstream of the relief valves and failure to provide emergency coolant injection. This would lead to a small loss of coolant, without the availability of emergency injection. The problem was corrected by changing the failure mode of some pneumatic valves in the heat transport system such that they failed closed on loss of this particular control power.

(b) The motorized isolation valves in the flow paths used to supply water to the steam generators following a reactor shutdown were all supplied from the same MCC. A design change was made such that the isolation valves in the flow paths to two steam generators in each reactor cooling loop were powered from different MCCs.

(c) A pneumatic valve in the cooling water supply to each boiler feed pump was opened only if all permitivies required to start the pump were met. Conversely, loss of any permitivie would lead to closure of the cooling water supply valve. It would not, however, lead to the feed pump tripping if already in the running state. A running main boiler feed pump would, therefore, operate without its cooling water supply and hence suffer damage unless turned off by the operator. The control system logic was corrected to prevent this.

(d) The location of radiation monitors in the reactor vault is such that closure of any of four valves would result in the monitors being bypassed undetected and failing to isolate containment on high radiation in the event of a release into containment (although isolation on high vault pressure would still occur). A change was made to provide alarms in the main control room to promptly detect and current incorrect valve position.

A major reason for identifying these deficiencies was the extent of the fault tree modelling, and the fact that the DPSE study was initiated more in response to a design verification need than to solely licensing demands. And, hence, led the analysts to take a more critical view of the design. Also, because most of the design of the station has been carried out within Ontario Hydro, the system analysts had ready access to the designers in order to confirm the validity of their concerns and proposed modifications.

**FUTURE ACTIVITIES**

The DPSE study report is scheduled to be issued by the end of 1986. It will be submitted to the regulatory authority as part of the documentation to be provided to obtain an operating license. It is anticipated that the information generated during the study will be of help in making decisions on safety-related issues during the operation of the plant.
REFERENCES


REVISION OF GENTILLY 2
SAFETY DESIGN MATRIX STUDIES

BY

R. Comeau (Hydro-Québec, Canada)
T. Schaubel (Atomic Energy of Canada Ltd, Canada)
K. Serdula (Serdula Systems Ltd, Canada)

Paper presented at:

ABSTRACT:

Hydro-Québec has recently completed the revision of three Safety Design Matrix studies on its Gentilly 2 nuclear power station (CANDU - PHW 600 MW). Using probabilistic techniques, these documents study the effects, from a safety point of view, of a complete loss of electrical supply, instrument air or service water system. The paper presents the outline of a SDM study, the reasons and results of the present revisions.

1. INTRODUCTION:

In Canada, at the present time, nuclear power plant licensing and safety requirements demand that the owner of a nuclear power station demonstrate the safety of its plant by accident analyses based on two different types of methodology which are:

- deterministic approaches,
- probabilistic developments.

The deterministic studies should prove the adequacy of the plant design by the confirmation that, on occurrence of specific accidents from fixed plant states, maximum radioactivity release criteria are respected.

The probabilistic studies, known as Safety Design Matrix studies, should demonstrate that the event sequences, which develop the responses of the plant to specific initiating events, end in either a stable plant condition (in which there is adequate fuel heat removal capability), or an incredible frequency (criterion: ≤ 10^-7 event/year) of significant release of radioactivity to the public.

Hydro-Québec has recently completed the revision of three Safety Design Matrix studies on its Gentilly 2 (CANDU-PHW 600 MW) nuclear power station. This station has been in commercial operation since 1983.

This paper presents the outline of a SDM study, the reasons for revising these studies and results of these revisions.

2. OUTLINE OF SDM STUDY:

A SDM study is developed around two main aspects: evaluation of the frequency of an initiating event and analysis of the response of the plant to this perturbation.

The first aspect is covered in the sections that present a brief description of the process system to be studied, analysis of its different failure modes, and, based on fault tree methodology, an evaluation of the probable frequencies of these process system failure modes (Figure 1).

The sections of the document that deal with the analysis of the plant response to the initiating event include the following:

- analysis of the effects of the process system failure on the other systems of the plant. This information is used to define an expected plant condition at the time of failure.
alarms and indications that will be available to the operator to diagnose the event and specified actions by the operator to mitigate consequences of the event.

- Development of event sequence drawings representing the most probable event scenarios arising from the initiating event. These event sequences take into account the unavailability of mitigating systems and unreliability of operator's action (Figure 2).

3. REASONS FOR THE REVIEW:

Although the SDM studies have been already submitted for the initial operating licence of Gentilly 2, Hydro-Québec took the decision to review three of those initial studies:

- Total Loss of Class IV Electrical Power,
- Total Loss of Service Water System,
- Total Loss of Instrument Air Supplies.

The decision to review these studies was based on the following reasons:

- the three systems (air supplies, electrical power and service water) provide common services to many process and safety-related systems and their unavailability impacts significantly on the performance of many other systems;
- the number and importance of modifications done during commissioning as well as the observations made during early operation dictated that these three initial studies should be revised systematically to validate the agreement with the as-built plant;
- the verification of the realism of expected operators' responses.

4.0 RESULTS OF REVIEW:

4.1 Initiating event frequencies

In the initial stages of the revision it was found that consideration of details not included in the original studies and the reflection of the as-built conditions and existing operating procedures resulted in net increases in probable frequencies of the initiating events. Major contributors to these increases were identified from the fault trees. Based on this information minor modifications to systems and operating procedures were recommended and implemented.

Identified modifications can be illustrated by the example of a limitation on service water system operating characteristic which was found to have a significant impact on the frequency of the total loss of the system.

By design intent, two raw cooling water pumps were to be in operation during the winter period to cool the recirculated service water. Operating experience had demonstrated that the required number of raw cooling water pumps in operation should be reduced to only one to avoid an overcooling of the recirculated service water that could result in possible freezing of the water in some heat exchangers.

In this latter operating configuration, the failure of only one running raw cooling water pump could have caused a complete loss of the service water system. The review illustrated that the reliability of the system, in this configuration, could be improved by the addition of a "standby" position to the starting logic of the pump. This modification was implemented and is reflected in the final fault tree.

It should also be mentioned that inclusions of some other operating characteristics, such as a reduction of the winter operating period, to reflect experience, has contributed also to a decrease of the frequency of the initiating event.

The systematic revision of the fault trees has provided the opportunity to assess existing test frequencies of the equipment studied. This resulted not only in a few testing frequencies being increased, but also in some being decreased when the effect was negligible. It was also found that a few tests of inactive standby equipment have not been formally implemented into the site routine test program.

The systematic revision of the fault trees has shown that some of these were not adequately developed. These fault tree revisions resulted in the addition of some failure modes and in the modification of the frequency of already considered failure modes. Those modifications have significantly affected, for example, the results of the loss of electrical power study.

In summary, incorporation of many changes to expand the initial studies and to reflect the as-built conditions and operating procedures resulted in initial net increases in probable frequencies of the initiating events. However, implementation of minor modifications to systems and operating procedures identified in the revision process has resulted in the final derived values of the probable frequencies of the initiating events of about the same magnitude as those in the initial reports. In fact the probable failure frequency was decreased by a factor of two for one system and increased by factors of 1.5 and 2.0 for the other two systems.
4.2 Event sequences

The detailed revision of event sequences has improved the information available on plant responses to some initiating events.

Consideration of the as-built system operating characteristics and requirements of the operating documentation has modified the number and the frequency of event scenarios.

The initial studies have often used the "worst case" concept to develop some scenarios. Although this approach is generally conservative, it does not describe adequately the real response of the plant and, in some cases, it could even suggest some unneeded modifications. The revised studies have introduced, in some event sequences, intermediate situations and their respective probabilities of occurrence.

4.3 Operators' role

In the development of event sequences, the operators' role is of prime importance not only to mitigate the effect of the failure of an expected automatic system response, but also to assure a long term heat sink for the reactor.

The realism of the expected operators' actions to mitigate the consequences of an initiating event was verified not only by an analysis of available alarms and indications but also taking into account local and ease of intervention as well as site normal and abnormal operating procedures.

The review process has brought to light an aspect of the actual operator model where further development would be beneficial: the maximum allowable credit for operator actions in one event sequence. In fact, even if all indications, mitigating systems and many hours are available for an operator action, the maximum credit criterion (≤ 10^2) can be a questionable limit in the development of a long event sequence leading to long term heat sink.

4.4 Cross-link analysis

The revised studies put emphasis on the origin of potential cross-links among the loss of the three studied systems. It was brought out, for example, that a simple action such as a manual start of the travelling screens at the pumphouse, during a loss of instrument air, can prevent their blockage and a consequential loss of service water. In fact, an automatic start of those screens is prevented, during a loss of instrument air, by the unavailability of the differential pressure measurement.

4.5 Tool for training and operating

The information level, in the original study, was adequate for design and licensing purpose, but because of its general descriptions was not a valued reference for training or operating staff. During the review process, only minor efforts were required to incorporate additional details and explanations that have greatly improved the system descriptions as well as the understanding of their interactions with other systems.

4.6 Effect on station availability

The revision of the three SDM studies, dealing with failures of the three common service systems, was undertaken mainly for safety considerations.

However, it happens that almost every modification done to decrease the probability of failure of one of those systems and thus improve safety, also enhances simultaneously the availability of the plant.

The fault trees' revision provided the opportunity to review and revise some repair time values in accordance with site experience and procedures. In some cases, it was shown that operating constraints can be decreased by a reevaluation of the maximum allowable repair time.

For example, to limit the probability of a class IV electrical power loss during reactor operation, the plant operating policy states the reactor should be shutdown if it is estimated that the station service transformer will be unavailable for more than eight hours. The revision of the studies has indicated that even if the duration was extended to twenty-four hours, the frequency of loss of Class IV was not affected significantly.

5. CONCLUSION

The inclusion, in the three revised Safety Design Matrix studies, of the as-built changes to the plant, the expansion of detail of some parts of the initial versions, and the addition of the operating systems characteristics, has significantly affected the results of the evaluation of some event sequences' frequencies.

During the revision, the established assessment methodology was used not only to calculate the impact of the changes on the safety of the plant, but also to identify modifications at the least cost to the plant which were able to reduce this impact. The design target of the probable failure frequencies of the three service systems was practically reached through implementation of only a few minor system modifications combined with some changes in equipment testing frequencies and operating modes.
Although fully aware of the limitations of probabilistic methodology, Hydro-Québec has tried, during the revision of the three SUM studies, to exploit the maximum potential of this tool. The revision task was not confined only to the risk assessment, its main purpose, but tried also to take advantage of the methodology to select modifications to improve plant availability and operation. Sufficient detail was also provided in the final study reports for their use as reference training and operating documentation.

REFERENCES

Information disclosed in this text was based on internal and proprietary documentation of Hydro-Québec and Atomic Energy of Canada Ltd.

FIGURE 1: FAULT TREE LOGIC TO ESTABLISH FAILURE FREQUENCY OF THE PROCESS FAILURE
Figure 2: Event sequence logic to establish plant responses.
1. Introduction

A fundamental basis for licensing a nuclear power plant is a confirmation of high reliability of safety systems and a high quality of equipment in order to avoid accidents.

For the verification of these statements several safety and reliability analyses and quality assurance measures are outlined in the licensing procedure of a plant.

By this concept, sufficient plant safety management for long term NPP operation will be necessary
- to keep the risk level of the plant over lifetime within acceptable boundaries.

The safety management is an integral part of the plant safety concept, established by
- hardware, as a multiple safety barrier and safety feature
- software, as an operating and test procedure system.

These safety elements are more or less assessed by deterministic requirements and improved and optimized by the use of probabilistic safety analysis (PSA).

Today in the FRG the PSA is well developed and used for the layout and supervision of safety systems in the design and the construction phase of a plant, e.g.
- to look for weak points in the safety design
- to optimize test and maintenance procedures
- to evaluate rare events in order to find out if additional measures are necessary.

A guidance and a standardisation of how to convert the objectives of PSA into plant management procedures are not as readily available.
When applying PSA we have to recognize that a PSA only describes the safety and reliability characteristics of NPP as a snapshot in time of the actual plant operation. The following parameters of risk:
- frequency of initiating events
- reliability and availability of safety features
- possible consequences
are currently influenced by various elements in both directions:
- early faults and wear of components
- different component loads caused by the operational process
- environmental factors
- quality of maintenance and of test procedures
- extent of preventive maintenance
- safety-relevant management decisions
- human factors, knowledge and training
- quality of written procedures
- plant specific hardware and software modifications.

This paper describes our experience on:
- how to convert and supervise the aspects and assumptions of PSA into plant operation, developed during NPP licensing procedures and
- how to use an optimal feedback for safety purposes.

2. Requirements of System Reliability

In several German Standards, reliability requirements of safety systems are mostly formulated by qualitative statements like - sufficiently reliable -.

The most important probabilistic requirement is contained in the NPP-Safety Criteria of the Federal Ministry of Interior /1/ presented here in a shortened form:

1. Incidents shall be avoided with sufficient reliability and additionally,

2. Safety features shall control incidents with sufficient reliability.

These two requirements have been fulfilled so as to adequately balance the safety concept and probabilistic methods shall be as well as possible in accordance with the current state of the art.

To meet these requirements, the important safety functions for most PWR and BWR in the FRG are assessed by PSA, e.g.
- emergency core cooling
- heat removal
- containment isolation
- shut down
in respect of the selected (dominant) incidents of
- large, medium or small LOCA
- emergency power case
- loss of heat sink.

The most common analytical method in use is the Fault Tree Analysis /8/.

The probability data are generic data and are taken over from literature, e.g. the American and German Risk Studies /2,3/. These data are updated by plant specific data.

The most important result of analysis is to draw a quantitative picture about the safety concept of NPP for a more detailed and deeper look into the plant safety functions.
Table 1 gives an insight into the analyzed spectrum of incidences of a modern German PWR. These analyses were assessed for the licensing of the NPP by the manufacture and, independently, by the TÜV Norddeutschland.

The objective of the evaluated numbers is to show the relative contributions of each sequence to meeting the above safety criteria in respect of a well balanced safety system.

Because of the relative judgement value, the absolute numbers and the inherent uncertainty of calculated numbers are less important here.

As a result of the analyses described above the emergency heat removal system of the secondary side of the PWR has been improved by additional hardware components.

Additionally, all surveillance test intervals of component and system functions - used as input data in the analyses - were evaluated and transferred to the plant procedure manuals (Table 2).

For a further completion of plant construction, a very detailed and comprehensive analysis of the reactor protection system (RPS) was assessed by the manufacturer and TÜV so as to prove the previous analyses' assumptions of input data on control components (Picture 1).

In this analysis all channels of the RPS were assessed. Because of new items in electronic devices (ED) a detailed Failure Mode and Effect Analysis of each ED became necessary.

The failure rates of ED were evaluated by the possibility of 6 failure modes of passive and active failures and in respect of the type of failure detection.

As a result of the analysis, the unavailability of some RPS channels had to be decreased by additional monitoring devices and by an increase of test frequencies.

Up till now the extent and the depth of PSA covering all safety relevant functions of an NPP are not fixed by safety standards in the FRG.

Today, in the FRG some activities are underway sponsored by the Federal Ministry of the Interior on how to use and precise PSA for safety evaluation of an NPP.

3. Reliability Parameters and Assumptions of PSA

The currently used probabilistic methods of Fault Tree and Event Tree Analysis (FTA, ETA) base on

- deterministic assumptions, describing the performance and the efficiency of component and system functions like
  - they are true or not true - and
  - a set of quantitative input parameters.

Deterministic Assumptions of PSA:

The efficiency of system functions describes the desired system capacity, e.g. the flow rate of a pump for heat removal or the strength of a passive structure due to a possible maximum load. The assessment of the efficiency is based either on conservative or on best-estimate calculations.

Over lifetime the system efficiency is being verified by surveillance tests.

In many cases a realistic test of the system function is not possible because of abnormal incident conditions being required. This gap is generally filled by theoretical analysis and additional preoperational incident simulation tests.

The most important example for this is the efficiency of the emergency core cooling system in case of LOCA.
This system efficiency is transformed into the PSA (FTA) simply by the parameters of e.g. 2 out of 4 or 1 out of 3 system train redundancy.

There are other examples of system functions which can hardly be tested under realistic incident conditions: e.g. the component behaviour under the load of incidents such as

- vibration
- shock waves by a pipe break or by a fast shut-off of a valve
- hydraulic flow load on a valve affecting its closing function
- temperature and humidity in the course of an incident
- dirt deposit by a LOCA into the containment sump and into the recirculation cooling water increasing the pump failure rate.

Additionally, in many cases the integral system function can be verified by multiple individual tests only. Because of different component functions and plant operation conditions, the ECCS of a PWR are tested by applying 23 different test procedures (pictures 3-6).

For this reason caution shall be taken to not overlook effects which may result from these interfaces. It is hardly possible to quantify such effects in a PSA.

The only way is to increase the test quality in the above sense and to use, as much as possible, additional information from the normal and abnormal plant operational process about system functions.

Examples are:

- Operational fluctuation of plant parameters (temperature, pressure, level) can be used to check the correct function of transmitters of protection systems

- transient events like plant shut down or loss of main heat sink have to be evaluated so as to see whether safety systems are correctly activated or if they should be activated e.g. by the process computer or the recorder outputs.

"As good as a new" Model:

The system's and component's state of

- intact or fault -

is modelled in PSA in a binary state process. That means that the system or components are either completely intact or completely faulty to a function required. These states are generally indicated by monitoring devices to the control-room staff only.

The components are considered "as good as new" after having been tested and undergone maintenance.

The operational experience shows that this assumption is only a rough approximation of the real technical behaviour of components.

Furthermore, it is not always trivial to identify the actual component state by the information available on monitoring devices or others.

For example, a test of sufficient closure of a check valve is difficult to monitor. It can be done by pressure monitoring and by additional leak rate tests.

For a clarification of the desired component state, the written test procedures should always contain the desired and limited conditions of component functioning and its tolerances by quantitative numbers, such as leak rate, flow rate, shut-off time, start-up time (picture 8).

In the same sense, selection of the adequate test procedures after a component deficiency and after maintenance are not
The best way to keep this uncertainty effect low is the one of using an adequate feedback of maintenance activities.

**Planned Operational Procedures** of safety systems are normally described in the technical specifications and operational manuals and are important preassumptions of system modelling in PSA. As far as the operator can influence these procedures e.g. to leave an inspected valve in its wrong position, there is of course a failure probability in doing so.

Because of the great variety of possible system procedure changes a clear description of all safety-relevant component and system functions and states is necessary, as well as a guidance for safeguarded maintenance procedures. In addition, sufficient knowledge by and training of the plant staff is compulsive.

**Quantitative Input Parameters of PSA:**

1. failure rates
2. failure frequency on demand
3. failure frequency on time
4. repair and maintenance time (the time of unavailability observed)
5. test intervals
6. mission time

The first four parameters are assessed by operational experience, Parameters 4 and 5 are based on administrative regulations, and 6 is problem-orientated.

Considering the theme envisaged in this paper, only one aspect of the quantitative parameters shall be stressed here: the importance of **periodical surveillance tests**.

By the common application of constant failure rates of components in PSA and based on the stand-by state of most safety components the unavailability \( \bar{U} \) is calculated as:

\[
\bar{U} = 0.5 \lambda t
\]

for low values of \( \bar{U} \).

There are of course additional contributions to \( \bar{U} \):
- repair and maintenance and
- the failure probability in the course of an actual demand.

We think this failure probability will be low and that it can be covered by the failure rate, because it is quite difficult to distinguish between both by operational experience. NUREG 2300 /4/ gives a similar explanation about the use of constant failure rates with respect to the experience of several new American PRA.

By the modelling of \( \bar{U} \) as described, the importance of surveillance test intervals is obvious.

Because of this, strict administrative regulations about test procedures and test intervals of all safety-related components have been established for NPP in the FPG.

In this aspect there are, on the one hand, advantages of a higher test frequency by detection in advance of a possible common cause failure and, on the other hand, disadvantages in respect to an earlier wear out of components and an increase of radiation exposure of test personell in special cases.

Under these aspects, an optimal test frequency will have to be found.
4. Implementation of Analyses of Assumptions and Reliability
Data in Plant and Operational Documentation

According to the requirements of German Regulatory and
Licensing Procedures of NPPs, operational manuals and inspection
documents on
- test procedures and test intervals
- safety-operational regulations of component state and
  allowed outage times (AOT)
have to be prepared by the manufacturer and by the Utility
and require the approval of the licensing authority.

The assumptions and input data of PSA prepared for the
licensing procedure are annexed to these documents.

Test Procedures and Test Intervals

The inspection documents of a Plant are contained in inspection
manuals according to the requirements of German Standard
KTA 1202. This manual is subdivided into:
- a General Inspection Plan
- an Inspection Procedure
- Inspection Records

The surveillance test intervals for most active system
functions, based on PSA (table 2), are laid down in the General
Inspection Plan (picture 4-6).

The Utility is responsible for the test performance and an
adequate management of time schedules. Generally, independent
Inspectors of TUV are involved in these test procedures e.g.
on a yearly time schedule. The inspector checks the test
results of the Utility and writes a test report for the
licensing authority.

A more detailed description of the inspection procedures
in the FRG is given in /5/. With respect to the importance
of test intervals and in order to limit the increase of
unavailabilities, a set of permissible tolerances of the
periodical test intervals is given (picture 7).

There are some practical aspects of test procedures for
unavailability reduction which form a part of the inspection
manual in general:

- Test intervals of redundant trains are mutually subjected
  shiftings e.g. 4-train systems with a 4 week-test interval
  should be tested weekly. By this system the maximum number
  of system unavailabilities will decrease and it will give
  the chance of earlier revealing of a common cause or common
  mode failure.

- Safety-important valves such as pressure relief valves
  or isolation valves shall be tested by additional inspection
  procedures to discover deficiencies in advance. For example,
  the easy workability of valves can be checked by decreasing
  the load of the actuator up to the point where the functioning
  of the valve stops working. In addition, the evaluation
  of the time for controlling the valve's opening and closing
  and the comparison of these times with previous tests can
  be used to prematurely discover possible deficiencies.

Safety Operational Regulations and Allowed Outage Times (AOT)
are written in the operational manual of a plant according
to the requirements of German Standard KTA 1201.

The most important aspect of this is a regulation of component
and system failures. Based on the requirement of the Single
Failure Criterium /6/, the formulation is as follows:

to adequately control all incidents to be considered, redundant
systems have to established for the possibility of
- one single failure and
- one train out for maintenance.
To meet this criterion the safety systems of German plants are designed by redundancy of \( n + 2 \), resulting in a \( 3 \times 100 \% \) or \( 4 \times 50 \% \) system capacity. To limit the system unavailability in the case of component failure or maintenance, the allowed outage times of components are fixed in the operational manual.

For a typical \( n + 2 \) - System AOT ranges between one week and up to 4 weeks. This varies from plant to plant and depends on the specific safety constructions.

In addition to AOT requirements as specified, and during maintenance on the defect train component, the time table of test procedures of the intact trains is to be shifted to some earlier setpoints, e.g., the next train will be tested after 4 days.

For \( n + 1 \) - Systems (e.g., the double valve system of an isolation system) the AOT is limited to 24 hours in general. A similar limitation applies to an \( n + 2 \) - System in the case of two train faults.

These AOTs are based on the deterministic principle and are verified by engineering's judgement and probabilistic calculations. The operational experience shows that there is only a low probability of an NPP having to be shut down by the requirements of AOTs. This means, that for most components the maintenance time will be less than one week.

The probabilistic assessment of maintenance contribution to an unavailability of a system is always easy if a PSA is readily available.

On the other hand, an adequate judgement of the acceptable increase of maintenance-caused unavailability is a difficult job, due to the relatively small effect on the NPP-risk as a whole.

In principle there are two possibilities of judgement:

1. Relative judgement:
   the increase of system unavailability should be limited by a factor \( F \) compared to system unavailability without maintenance.

2. Absolute judgement:
   the increase of plant risk should be limited in case of maintenance.

The first assessment is easy to apply and supplies well-defined numbers. The disadvantage is that this method produces shorter AOT for systems with higher reliability than for those with lower reliability for the same safety task.

Basically, the second assessment supplies risk-relevant numbers. In this case it has to be recognized that the change of risk by single maintenance is small compared to the long-term risk and to the uncertainty of risk. In addition, this concept is much more complicated to handle because a complete plant-specific PSA has to be available for comparison. Examples for the use of the second method are given in [7].

By the use of the risk-method we have to realize that the risk of NPP is characterized by a time-dependent risk profile. That can be illustrated by an extreme example of the two check valves in series in the trains of the low pressure injection system (LPIS) that are connected to the primary circuit of PWR (picture 3).

The probability of an internal breakdown of both check valves, the so-called Interfacing System LOCA - is very small e.g., \( 10^{-4} \times 10^{-4} = 10^{-8} \) (the numbers are taken from [2,3], in the German Risk Study/Phase B, this probability is judged smaller today).

If one of the valves fails during actual plant operation the risk will change by about 4 magnitudes during a further one year's plant operation.
In an actual event of the first valve failure the probability would be of less importance for a plant safety decision, because it is the possibility of the second failure that has to be considered. For this purpose the AGTs are fixed for different German plants and range between 5.5 - 100 h. Because of the complexity described, this standard is still under discussion.

5. Quality Assurance and Management Task on Safety Aspects during Plant Operation

The task of PSM is to keep the safety level of the plant over the lifetime of the man-machine system. For this task the safety characteristics of a plant will have to be clearly described in the plant manual, in accordance with the written safety requirements for plant control and supervision. The interactions of NPP and plant staff can be described by diversified activities which are currently updated by various internal and external aspects (picture 2).

The important safety aspects of management tasks are described here by the following examples:

- Control and supervision of plant parameters are important in the context of transient events and other changes of parameters so as to check how the safety systems respond.
- Adequate feedback of operational experience on hardware behaviour, e.g., failure frequency and common cause failures.
- The efficiency of activities of plant safety management.
in order to guarantee sufficient plant quality as far as
safety is concerned.

These diverse plant specific management tasks in a PSA can
hardly be expressed by quantitative numbers.

The evaluated plant specific component failure rates and
maintenance-caused system unavailabilities are in fact parameters
of the actual plant quality.

6. Plant Specific Data and System Reliability

Data feedback of operational experience are used
- to check the actual failure data due to an increase of
failure rates caused by early faults, wear and common
causes and to compare these data with expected values
of previous PSA
- to evaluate plant specific data to update the available
data set for optimization of plant procedures.

This activity of data feedback with the possibility of correction,
if necessary, can be described as a - regulating circuit
of system reliability - (picture 9, taken from /9/).

The reliability regulating circuit (RRC) illustrated is
valid for each plant state, from the construction phase up
to the operation phase.

By this the external data in the former phases change more
and more into plant-specific data, if the RRC-process will
be optimally applied. The experiences of other industries
show that the use of a reliability assurance program (RAP)
will result in a reduction of actual failure rates (picture
10, taken from /10/).

Our experience with the evaluation of NPP operation shows
that, generally, the plant-specific failure rates of components
in safety systems are comparable with the generic data used
in previous analyses (table 3).

Of course, also extreme values are possible, caused by various
plant-specific effects.

Based on this experience we believe that there is an inherent
uncertainty of failure rates, and that therefore it will
not be possible to obtain more certainty of failure rates
by gathering more field data.

For the rare events of common mode and passive component
failures, improved data will be possible in future by more
field data.

For the permanent management task of evaluating safety component
failures with respect to their importance, the following
failure classification will be useful:

1. The event has no influence on a safety-related function
   of a component.

2. The event indicates a drift fault of a desired function,
   the function in itself is still correct.

3. Loss of a component's function without an indication of
   common cause - single failure -.

4. Drift fault of more than one component with a common cause.

5. The increase of the component failure rate is bigger than
   the uncertainty expected.

6. Multiple component failures by common causes observed
   on different time-points e.g. in different test intervals.

7. Multiple component failures by common causes at the
   same time - common mode failure -.
Events of categories 1 - 3 are principally tolerable because of the layout of the plant's safety concept by redundant systems.

Events of categories 4 - 7 are safety-important, because in addition to the normal maintenance activities further measures will be necessary to eliminate a common cause.

To indicate the above mentioned events in advance a wider oversight of plant maintenance activities should be applied. Therefore, an efficient plant information and documentation system will be necessary for the purpose of plant quality assurance (QA).

The Utility has the responsibility for this QA. By contract with the licensing authority TÜV Norddeutschland are involved in reviewing the NPP operational experience in respect of safety and with an emphasis on

- results and efficiency of surveillance tests
- abnormal events as transients
- component failures and maintenance due to the possibility of common causes as described in the above classification list.

This review is compiled by TÜV in a yearly technical report to the licensing authority.

Literature:


/3/ Deutsche Risikostudie, Kernkraftwerke, Eine Untersuchung zu dem durch Störfälle in Kernkraftwerken verursachten Risiko, Verlag TÜV Rheinland, 1979


/6/ Bekanntmachungen des Bundesministers des Innern, Interpretationen zu den Sicherheitskriterien für Kernkraftwerke, Einzelfehlerkonzept, Grundsätze für die Anwendung des Einzelfehlerkriteriums vom 10.05.1984 (GMBI 1984, Nr. 13).


/8/ DIN 25424, Fehlerbaumanalyse, Methode und Bildzeichen, Teil 1, 9/81
<table>
<thead>
<tr>
<th>Event/incident</th>
<th>Frequency 1/a</th>
<th>Unavailability of Safety System 1/a</th>
<th>Frequency of Sequence 1/a</th>
</tr>
</thead>
<tbody>
<tr>
<td>large LOCA</td>
<td>3.10^{-4}</td>
<td>4.1.10^{-4}</td>
<td>1.6.10^{-7}</td>
</tr>
<tr>
<td>heat removal syst.</td>
<td></td>
<td>1.3.10^{-4}</td>
<td></td>
</tr>
<tr>
<td>containment isolat.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>medium LOCA</td>
<td>8.10^{-4}</td>
<td>5.4.10^{-4}</td>
<td>4.3.10^{-7}</td>
</tr>
<tr>
<td>small LOCA</td>
<td>3.10^{-3}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>small leak to</td>
<td>2.10^{-3}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pressurizer valve</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>primary-side</td>
<td></td>
<td>5.4.10^{-4}</td>
<td></td>
</tr>
<tr>
<td>secondary-side</td>
<td></td>
<td>1.10^{-9}</td>
<td></td>
</tr>
<tr>
<td>emergency power case</td>
<td>3.10^{-2}</td>
<td>5.10^{-5}</td>
<td>1.5.10^{-6}</td>
</tr>
<tr>
<td>SG-tube leak</td>
<td>1.10^{-2}</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>external events *)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>heat removal syst.</td>
<td></td>
<td>3.10^{-3}</td>
<td></td>
</tr>
<tr>
<td>Primary circ.isol.</td>
<td></td>
<td>4.6.10^{-3}</td>
<td></td>
</tr>
<tr>
<td>Loss of main feed water</td>
<td>4.10^{-1}</td>
<td>1.10^{-5}</td>
<td>4.10^{-6}</td>
</tr>
<tr>
<td>Leak in second. circ.</td>
<td>3.10^{-3}</td>
<td>1.10^{-3}</td>
<td>3.10^{-6}</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>1.2.10^{-5}</td>
<td></td>
</tr>
</tbody>
</table>

*) only qualitative assessment by comparing other events
Table 2: Surveillance Test Intervals assessed by PSA

<table>
<thead>
<tr>
<th>System</th>
<th>Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency core cooling system</td>
<td>4 w</td>
</tr>
<tr>
<td>Nuclear component cooling system</td>
<td>4 w</td>
</tr>
<tr>
<td>Service cooling water system</td>
<td>4 w</td>
</tr>
<tr>
<td>Check valves to primary circuit</td>
<td>1 a</td>
</tr>
<tr>
<td>Pressurizer-blowdown isolation valve</td>
<td>8 w</td>
</tr>
<tr>
<td>- blowdown valve</td>
<td>1 a</td>
</tr>
<tr>
<td>Containment isolation valves</td>
<td>1 a</td>
</tr>
<tr>
<td>Volume control system</td>
<td>1 a</td>
</tr>
<tr>
<td>ECCS</td>
<td>4 w</td>
</tr>
<tr>
<td>Nuclear ventilation system</td>
<td>4 w</td>
</tr>
<tr>
<td>Nuclear building drain system</td>
<td>4 w</td>
</tr>
<tr>
<td>Nuclear component cooling system</td>
<td>1 a/4 w</td>
</tr>
<tr>
<td>Fuel element storage pool cooling system</td>
<td>4 w</td>
</tr>
<tr>
<td>Emergency heat removal system second, side</td>
<td>4 w</td>
</tr>
<tr>
<td>Check valves to SG</td>
<td>1 a</td>
</tr>
<tr>
<td>Emergency power supply</td>
<td>4 w</td>
</tr>
<tr>
<td>Start-up and shut-down of cooling system</td>
<td>3 m</td>
</tr>
<tr>
<td>Volume control system spray valve</td>
<td>4 w</td>
</tr>
<tr>
<td>Steam dump valves</td>
<td>1 a</td>
</tr>
<tr>
<td>Primary isolation valves</td>
<td>1 a</td>
</tr>
</tbody>
</table>

\(a = \) annually  
\(m = \) monthly  
\(w = \) weekly

---

Table 3: Comparison of Failure Rates of ECCS-Pumps based on Operational Experience and Generic Data

<table>
<thead>
<tr>
<th>ECCS-Pumps</th>
<th>Failure Mode</th>
<th>Failure Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Plant 1</td>
<td>Plant 2</td>
</tr>
<tr>
<td>HPIP</td>
<td>stand by</td>
<td>fails to start</td>
</tr>
<tr>
<td>LPIP</td>
<td>low operat.</td>
<td>fails to start</td>
</tr>
<tr>
<td>NCCS-P</td>
<td>high operat.</td>
<td>fails to operate</td>
</tr>
<tr>
<td>SCWS-P</td>
<td>high operat.</td>
<td>fails to operate</td>
</tr>
</tbody>
</table>

HPIP - High pressure injection pump  
LPIP - Low pressure injection pump  
NCCS-P - Nuclear component cooling water system-pump  
SCWS-P - Service cooling water system-pump
Picture 1: Basic Construction of Component Control Circuit

Picture 2: Safety Information System of Plant Staff
### General Inspection Plan for the Emergency Cooling and Residual Heat Removal System

<table>
<thead>
<tr>
<th>Plant</th>
<th>Date/Time</th>
<th>GENERAL INSPECTION PLAN</th>
<th>Operational Condition</th>
<th>Copy</th>
<th>State</th>
<th>Sheet of</th>
</tr>
</thead>
<tbody>
<tr>
<td>YZ</td>
<td>2.4.1</td>
<td>functional test high-pressure injection</td>
<td>1a 1) i a x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>YZ</td>
<td>2.4.2</td>
<td>functional test low-pressure injection signal YZ 30 from termination element</td>
<td>1a 1) i a x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>YZ</td>
<td>2.4.3</td>
<td>functional test emergency cooling preparation signal YZ 31 from termination element</td>
<td>1a 1) i a x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>YZ</td>
<td>2.4.4</td>
<td>functional test flood signal YZ 45-46 from termination element</td>
<td>1a 1) i a x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>YZ</td>
<td>2.4.5</td>
<td>functional test sump signal YZ 41-44 from termination element</td>
<td>1a 1) i a x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TH</td>
<td>2.4.6</td>
<td>functional test of high-pressure injection pumps TH 15-45 DO01</td>
<td>1a 1) i a x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TH</td>
<td>2.4.7</td>
<td>functional test three-way-valve TH 15-45 BO06</td>
<td>1a 1) i a x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TH</td>
<td>2.4.8</td>
<td>functional test of residual heat removal pumps TH 10-40 DO01</td>
<td>1a 1) i a x</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1) one redundancy each week

---

**Note:**
- **GIP** = General Inspection Plan
- **IP** = Inspection Procedure
- **U** = Utility
- **I** = Independent Inspector

---

**Diagram:**
- Emergency Cooling and Residual Heat Removal System
- 1 Flood Tank
- 2 Accumulator
- 3 Residual Heat Removal
- 4 Residual Heat Exchanger
- 5 High-Pressure Injection Pump
- 6 Three-Way-Valve

---

### Diagram Details

- **TA:** Test Line
- **Sump:** Location of sump for heat removal
- **3:** Valves and control points for system integration
### GENERAL INSPECTION PLAN

<table>
<thead>
<tr>
<th>Date/Legibility</th>
<th>Operational Condition</th>
<th>Copy</th>
<th>State</th>
<th>Sheet of</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGP/IP Nr.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Topic (mode of testing, testing procedure, component, redundancy)</td>
<td>Test interval</td>
<td>U</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>2.4.9</td>
<td>Functional test of check valves TH 10-40 BOC35 at the flood tanks</td>
<td>1m</td>
<td>1a</td>
<td>X</td>
</tr>
<tr>
<td>2.4.10</td>
<td>Functional test of initial isolating valves at the accumulators TH 16-46 BOC1/BOC2</td>
<td>6m</td>
<td>1a</td>
<td>X</td>
</tr>
<tr>
<td>2.4.11</td>
<td>Functional test of initial isolating valves TH 12-42 BOC6 TH 21-41 BOC2 at the loops</td>
<td>1m</td>
<td>1a</td>
<td>BE-W BE-W</td>
</tr>
<tr>
<td>2.4.12</td>
<td>Functional test of pressure switches, checking of nitrogen pressure in the double-walled sump line</td>
<td>1a</td>
<td>1a</td>
<td>X</td>
</tr>
<tr>
<td>2.4.13</td>
<td>Functional test of safety features against exceeding of pressure</td>
<td>4a</td>
<td>4a</td>
<td>X</td>
</tr>
<tr>
<td>2.4.14</td>
<td>Test of heat removal capacity of the hooked-up NHR cooling chains</td>
<td>1a</td>
<td>1a</td>
<td>X</td>
</tr>
<tr>
<td>2.4.15</td>
<td>Sampling with chemical analysis of the boron acid concentration in flood tanks TH 10-40 BOC1</td>
<td>1m</td>
<td>2a</td>
<td>X</td>
</tr>
</tbody>
</table>

*** CCS = component cooling system
NCSWS = nuclear service cooling water system

---

### GENERAL INSPECTION PLAN

<table>
<thead>
<tr>
<th>Date/Legibility</th>
<th>Operational Condition</th>
<th>Copy</th>
<th>State</th>
<th>Sheet of</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGP/IP Nr.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Topic (mode of testing, testing procedure, component, redundancy)</td>
<td>Test interval</td>
<td>U</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>2.4.16</td>
<td>Sampling with chemical analysis of the boron acid concentration in accumulators TH 16-46 BOC1</td>
<td>1m</td>
<td>2a</td>
<td>X</td>
</tr>
<tr>
<td>2.4.17</td>
<td>Visual inspection of the system with checking the operating position of valves</td>
<td>1m</td>
<td>1a</td>
<td>X</td>
</tr>
<tr>
<td>2.4.18</td>
<td>Leakage test of residual heat removal system including sump line under operating pressure</td>
<td>1a</td>
<td>1a</td>
<td>X</td>
</tr>
<tr>
<td>2.4.19</td>
<td>Non-destructive testing (US/SC) of the accumulators TH 16-46 BOC1</td>
<td>4a</td>
<td>4a</td>
<td>X</td>
</tr>
<tr>
<td>2.4.20</td>
<td>Visual inspection (internal) of the accumulators TH 16-46 BOC1</td>
<td>4a</td>
<td>4a</td>
<td>X</td>
</tr>
<tr>
<td>2.4.21</td>
<td>Non-destructive testing (US/SC) of the piping</td>
<td>4a</td>
<td>4a</td>
<td>X</td>
</tr>
<tr>
<td>2.4.22</td>
<td>Pressure test of residual heat removal coolers TH 10-40 BOC3</td>
<td>8a</td>
<td>8a</td>
<td>X</td>
</tr>
<tr>
<td>2.4.23</td>
<td>Visual inspection (internal) of the residual heat removal coolers TH 10-40 BOC3</td>
<td>4a</td>
<td>4a</td>
<td>X</td>
</tr>
</tbody>
</table>

*** CCS = component cooling system
NCSWS = nuclear service cooling water system
US = ultrasonic
SC = surface crack
### GRS - MODEL OF PERMISSIBLE TOLERANCES OF INSPECTION INTERVALS OF PERIODICAL INSPECTIONS

<table>
<thead>
<tr>
<th>INSPECTION INTERVAL</th>
<th>TOLERANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEEKLY (1 w)</td>
<td>±2 DAYS (2 d)</td>
</tr>
<tr>
<td>2 WEEKLY (2 w)</td>
<td>±4 DAYS (4 d)</td>
</tr>
<tr>
<td>MONTHLY (1 m)</td>
<td>±8 DAYS (8 d)</td>
</tr>
<tr>
<td>3 MONTHLY (3 m)</td>
<td>±16 DAYS (16 d)</td>
</tr>
<tr>
<td>6 MONTHLY (6 m)</td>
<td>±1 MONTHS (1 m)</td>
</tr>
<tr>
<td>YEARLY (1 a)</td>
<td>±2 MONTHS (2 m)</td>
</tr>
<tr>
<td>2 YEARLY (2 a)</td>
<td>±4 MONTHS (4 m)</td>
</tr>
<tr>
<td>3 YEARLY (3 a)</td>
<td>±5 MONTHS (5 m)</td>
</tr>
<tr>
<td>≥4 YEARLY (4 a)</td>
<td>±6 MONTHS (6 m)</td>
</tr>
</tbody>
</table>

**Utilization of a tolerance does not change the due date of the next periodical inspection.**

---

**Picture B:** Example for the checkbacks and the controls to be performed on the basis of an inspection procedure concerning the functional test of the high-pressure injection pump (excerpt).

<table>
<thead>
<tr>
<th>Component</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inspection</td>
<td></td>
</tr>
<tr>
<td>1 YZ 36</td>
<td>Press the test key. on</td>
</tr>
<tr>
<td>1 YZ 36</td>
<td>Trip signal red</td>
</tr>
</tbody>
</table>

**Checkbacks**

<table>
<thead>
<tr>
<th>Component</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 TH 15 DO02</td>
<td>Oil pump high-pressure injection pump on</td>
</tr>
<tr>
<td>1 TH 15 DO03</td>
<td>Oil pump high-pressure injection pump on</td>
</tr>
<tr>
<td>1 TH 15 DO01</td>
<td>High-pressure injection pump on (5 sec. delayed)</td>
</tr>
</tbody>
</table>

**Record service point 1 of pump characteristic curve concerning feed-in "cold leg"**

<table>
<thead>
<tr>
<th>Component</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 TH 51 SO01</td>
<td>open</td>
</tr>
<tr>
<td>1 TH 51 SO02</td>
<td>open</td>
</tr>
<tr>
<td>0 TH 15 PO01</td>
<td>target:... (bar) actual:... (bar)</td>
</tr>
<tr>
<td>0 TH 15 PO02</td>
<td>target:... (bar) actual:... (bar)</td>
</tr>
<tr>
<td>0 TH 15 FO01</td>
<td>target:... (m/秒) actual:... (m/秒)</td>
</tr>
</tbody>
</table>

**Record service point 2 of pump characteristic curve concerning feed-in "hot leg"**

<table>
<thead>
<tr>
<th>Component</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 TH 51 SO01</td>
<td>open</td>
</tr>
<tr>
<td>1 TH 51 SO02</td>
<td>closed</td>
</tr>
<tr>
<td>0 TH 15 PO01</td>
<td>target:... (bar) actual:... (bar)</td>
</tr>
<tr>
<td>0 TH 15 PO01</td>
<td>target:... (bar) actual:... (bar)</td>
</tr>
<tr>
<td>0 TH 15 FO01</td>
<td>target:... (m/秒) actual:... (m/秒)</td>
</tr>
</tbody>
</table>

**Record zero-delivery head (pump delivers minimum)**

<table>
<thead>
<tr>
<th>Component</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 TH 51 SO01</td>
<td>closed</td>
</tr>
<tr>
<td>1 TH 51 SO02</td>
<td>closed</td>
</tr>
<tr>
<td>0 TH 15 PO01</td>
<td>target:... (bar) actual:... (bar)</td>
</tr>
<tr>
<td>0 TH 15 PO02</td>
<td>target:... (bar) actual:... (bar)</td>
</tr>
</tbody>
</table>

**Remark**

By the changeover of the test armatures, the tree-way-valve will be tested as well.
Picture 9: Regulating Circuit of System Reliability
The use of PSA techniques in a CEGB power station operational environment

Dr. B. E. Horne
CEGB
Generation Development and Construction Division

Abstract

The operation of a nuclear power station requires that safety objectives are adequately satisfied in order to assure the safety of the operators and the general public. For these safety objectives to be satisfied, the essential systems of a nuclear power station are installed and operated with considerable redundancy in plant and equipment. It is a necessary requirement that in the presence of faults or outages of plant due to maintenance this redundancy is always maintained at an acceptable level.

The essential systems of a nuclear power plant are large, complex and inter-related. Different essential systems contain different levels of redundancy of plant, depending on the reliability requirements for the essential functions provided. Plant outages in these systems require careful control to ensure that levels of plant redundancy in these systems are always above the specified minima.

Traditionally in the United Kingdom, the minimum levels of plant redundancy in each essential and supporting system have been stipulated to operational staff in concise and unambiguous instructions. However, because of the requirement for conciseness, and the inherent complexity and inter-relation of the essential systems when considered as a whole, these instructions have interpreted the requirements for minimum levels of plant redundancy in ways which are pessimistic. The instructions have been based on deterministic fault tolerance criteria applied on a system by system basis.

The extensive experience within CEGB of PSA techniques, in particular in fault tree analysis techniques, suggested the possibility of applying some probabilistic methods to the derivation of these operating instructions. An extensive programme of software development was therefore initiated to provide a fault tree model of the essential systems plant which could be assessed interactively from the Central Control Room as an operational aid, and from the planning office as a maintenance planning aid. The fault tree model had to be capable of being continuously updated to accommodate plant outages and plant changes as they occurred.

The development of this software has been completed (Ref. 1) and the facility, known as the Essential Systems Status Monitor (ESSM) has been installed on a dedicated mini computer at Heysham B Nuclear Power Station. The commissioning tests have been planned to be completed mid 1986.

This paper briefly reviews the development of the ESSM and then discusses its proposed operational use and the underlying safety philosophy principles.
2. DEVELOPMENT OF THE ESSM FACILITY

2.1 Objectives

An overall objective in the development of the ESSM was to provide a facility which allowed the basic probabilistic principles on which the Safety Case is based to be incorporated into the operational features of the essential systems of a power station. The facility was therefore required to assess the integrity of all of the essential systems and to assess then in relation to the functional requirements arising from all the relevant initiating faults included in the Safety Report.

For the ESSM to be suitable as an operator aid the facility was required to be interactive, and to be able to assess the effects of all possible combinations of plant outages and plant configurations. Having made an assessment of the particular operational situation, then the facility was also required to provide the operator with advice on what plant should be re-instated to an operational state from a maintenance state in order to improve the overall integrity.

Other features, such as the provision of a planning facility which was separate from the operational assessment facility, evolved during the development phase of the ESSM. Special security arrangements required for this type of facility also evolved during the development phase, and it was a design objective that the ESSM should be accommodated on a dedicated mini computer at the Station.

2.2 Design Development

The design of the ESSM facility is shown in Figure 1. The software has been developed on a Honeywell DPS6/92 machine, and an IBM mainframe machine, with the software written in FORTRAN 77. The size of the machine required to run the ESSM is basically a function of the size of the input fault trees.

There are 2 distinct software modules, the 'pre-processor' and the 'interactive' module. The 'pre-processor' is responsible for checking the input data files which define the fault trees, item probabilistic failure data, initiating events and plant configuration details. In addition, the 'pre-processor' is responsible for coding the input data into a form ready for use by the 'interactive' module. The 'interactive' module is responsible for providing the main functions of the ESSM, namely the integrity assessment and maintenance priority functions. The 'pre-processor' module can only be accessed by personnel with the necessary security clearance and is used infrequently (e.g. to make modifications to the original fault tree structure). The 'interactive' module is accessed by the operators and is in continual day-to-day use. Facilities are provided within the 'interactive' module of the ESSM to allow the operator to enter the current status of the essential systems. The operator informs the ESSM that various plant items are unavailable due to faults or preventive maintenance. In addition, the operator may input system configuration changes to the ESSM. The ESSM reconfigures and re-evaluates the effects of such outages and configuration changes on the original basis fault trees.

Special highly efficient and fast analytical methods were developed for the ESSM to enable it to be interactive. The minimal cut-sets for the fault tree representing all the essential systems are evaluated taking into account the logical effect of plant outages and plant configurations. The ESSM does not work by modifying previously calculated lists of minimal cut-sets, but re-calculates the minimal cut-sets for each assessment. This is essential to the accuracy of the ESSM.

Fault trees modelling the eleven essential and supporting systems listed in Table 1 and the eight groups of initiating events shown in Table 2 are contained in the formatted plant data files of the ESSM. Data for the frequencies of the initiating events and failure data for components are also contained in the files. These are all used for the probabilistic assessments carried out by the ESSM.

Also contained in the data files are logic modules of the "back stop rules". These rules describe the overriding deterministic criteria for the plant availability conditions for which a controlled reactor shutdown is required.

3. USE OF THE ESSM IN AN OPERATIONAL ENVIRONMENT

3.1 Control Room Facilities

The facilities provided in the Control Room of the power station for operating the ESSM consist of two computer terminals with VDU's, one for each reactor, and one hard copy printer.

The ESSM is a menu driven facility in which the operator selects options from successive menus for the precise function he requires.

The interactive functions of the ESSM provide:

1. Information on the current status of the options following plant failures, or on a future status if plant is taken out of service;
2. the capability to re-configure the system fault tree models either to model existing conditions or to model future planned plant outages;
3. information on the most effective options for plant replacement which will improve the status of the systems.

The information on current status is displayed to the operator in terms of one of three conditions: 'normal maintenance', 'urgent maintenance', or 'immediate remedial action', as shown in Figure 2. Precise probabilistic information is not displayed. Although the condition of 'immediate remedial action' may be displayed by the ESSM the operator would not normally use this as a basis for initiating a reactor shutdown since he is always required independently to confirm that the system status is consistent with the limits of the overriding simple deterministic rules as contained in hard copy form in the Control Room. The ESSM does also incorporate these limiting deterministic rules within its modelling so that before any probabilistic assessment is carried out the ESSM first checks that the system status satisfies these rules.
Having completed an assessment of the status of the essential systems, the ESSM may then be used to provide information on the optimum combinations of plant for restoration from unavailability conditions which could improve the overall integrity of the systems. This information is provided in the form of advice to the operator so that other factors not available to the ESSM, such as availability of maintenance personnel, may be taken into account in adopting the most appropriate action.

The hard copy printer in the Central Control Room is provided so that every time the plant availability conditions of the essential systems are changed then a record of this is made in hard copy format. This is expected to be of particular use at the beginning of an operator shift, and for providing a record of the system changes.

5.2 Maintenance Planning Facility

The facility for using the ESSM for advice on maintenance planning is provided on a separate terminal located in the planning office.

For this facility the ESSM generates a separate fault tree model to that used by the control room operator so that the planning office does not access the fault trees modelling the current status of the systems. This facility therefore allows future outages of plant to be modelled and assessed. This allows an operator to plan the outages of plant necessary for scheduled maintenance so that coincidences of plant unavailabilities have a minimal effect on overall system integrity.

3.3 Operational Principles

The probabilistic integrity assessments provided by the ESSM are system assessments summated over all the initiating events in turn factored by their estimated frequencies of occurrence. An overall frequency of failing to achieve defined minimum success criteria is therefore calculated which is similar to that derived from a conventional PSA for the operation of the essential cooling systems following a reactor trip.

The integrity status of a particular system condition is assessed by comparing this overall risk frequency figure with fixed pre-set frequency levels, typically one decade apart. The system status is thereby defined in one of the three conditions shown in Figure 2.

Traditionally system status has been defined in terms of the ability of individual systems to tolerate faults. Typically 'normal maintenance' could have been defined as the ability of a system to tolerate two active faults, and 'urgent maintenance' as the ability to tolerate one active fault. A whole range of overall plant unavailability conditions were therefore defined in terms of one of the three overall system status conditions depending on the abilities of the individual systems to tolerate faults. These conditions are normally defined in hard copy form and retained in the Control Room of a power station. In probabilistic terms these conditions can be represented by the irregular system status boundaries shown in Figure 3.

In principle the effect of using PSA techniques in operation, as provided by the ESSM could be to replace both of the irregular boundaries of overall system status shown in Figure 3 with the straight line boundaries shown in Figure 2.

In practice however it is proposed to define only one boundary on a probabilistic basis, i.e. the boundary between the 'normal' and 'urgent maintenance' operational conditions. It is proposed to retain a deterministic boundary between the 'urgent maintenance' and the 'immediate remedial action' operational states, as shown in Figure 4. This means that the ESSM will not be used to define the operational conditions requiring some immediate remedial action such as a controlled reactor shutdown. These conditions will continue to be defined primarily in hard copy form. The ESSM does not therefore form part of the basic safety instrumentation safeguarding the operational safety of the reactor.

4. CONCLUSIONS

This paper has summarised the principal features of the application of the PSA facilities provided by the Essential Systems Status Monitor to the operational environment of a commercial nuclear power station.

The ESSM is currently being used on a main frame computer in its operational form, and is to be commissioned on a mini computer at Heysham 'B' power station within a few months.

ACKNOWLEDGEMENT

This paper is published by permission of the Central Electricity Generating Board.

REFERENCE

Post trip sequencing equipment
Pressure support system
Start/standby boiler feed system
Emergency boiler feed system
Essential electrical system
Decay heat boiler feed system
Reactor sea water system
Inlet guide vane system
Gas circulators
Circulators auxiliaries cooling system
Circulators auxiliaries diverse cooling system

1. Spurious R-trip
2. Feed system faults
   Steam system faults
3. Water ingress faults
4. Primary coolant faults
5. Reactivity faults
6. Loss of grid connection faults
7. Depressurisation faults
8. Faults in essential systems

Table 1  ESSM — Essential systems modelled

Table 2  ESSM — Initiating events modelled
GERMAN PRECURSOR STUDY
REASONS FOR THE REFERENCE
PLANT BIBLIS

- Technical lay-out of Units A and B is very similar.
- Longest operating experience of all German NPPs.
- Most representative plant for the German PWRs, which are now operating or are to be licensed.
- Detailed information about the operating experience was available.
- Event trees and fault trees of the German Risk Study could be used.
- The results are directly comparable with the results of the German Risk Study.
### FREQUENCIES OF INITIATING EVENTS

<table>
<thead>
<tr>
<th>Event</th>
<th>German Precursor Study</th>
<th>German Risk Study</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of main feedwater</td>
<td>1.1/yr</td>
<td>0.8/yr</td>
</tr>
<tr>
<td>Loss of preferred power:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unit A</td>
<td>0.5/yr</td>
<td>0.1/yr</td>
</tr>
<tr>
<td>Unit B</td>
<td>0.1/yr</td>
<td></td>
</tr>
<tr>
<td>Demand of pressurizer relief valves</td>
<td>1.0/yr</td>
<td>0.6/yr</td>
</tr>
</tbody>
</table>

### TRAIN UNAVAILABILITIES

<table>
<thead>
<tr>
<th>Event</th>
<th>German Precursor Study</th>
<th>German Risk Study</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFWS</td>
<td>$1.7 \times 10^{-2}$</td>
<td>$3.2 \times 10^{-2}$</td>
</tr>
<tr>
<td>ECCS: HPI</td>
<td>$4 \times 10^{-3}$</td>
<td>$2.4 \times 10^{-2}$</td>
</tr>
<tr>
<td>LPI</td>
<td>$1.8 \times 10^{-2}$</td>
<td>$2.9 \times 10^{-2}$</td>
</tr>
<tr>
<td>ACCI</td>
<td>$1.6 \times 10^{-4}$</td>
<td>$1.2 \times 10^{-2}$</td>
</tr>
<tr>
<td>Component Cooling System</td>
<td>$5 \times 10^{-4}$</td>
<td>$1.7 \times 10^{-2}$</td>
</tr>
<tr>
<td>Service Water System</td>
<td>$2 \times 10^{-3}$</td>
<td>$2.1 \times 10^{-2}$</td>
</tr>
<tr>
<td>Chilled Water System</td>
<td>$4 \times 10^{-3}$</td>
<td>$2.8 \times 10^{-2}$</td>
</tr>
<tr>
<td>Emergency Diesel System</td>
<td>$1.4 \times 10^{-2}$</td>
<td>$4.5 \times 10^{-2}$</td>
</tr>
</tbody>
</table>
GERMAN PRECURSOR STUDY
FREQUENCY OF THE EVENTS SELECTED AS PRECURSORS vs. OPERATING YEAR
$f(1/yr)$

<table>
<thead>
<tr>
<th>yr</th>
<th>75</th>
<th>76</th>
<th>77</th>
<th>78</th>
<th>79</th>
<th>80</th>
<th>81</th>
<th>82</th>
<th>83</th>
</tr>
</thead>
<tbody>
<tr>
<td>f(1/yr)</td>
<td>10</td>
<td>9</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

- all precursors
- precursors with contributions from human error

GERMAN PRECURSOR STUDY
FREQUENCY OF POTENTIAL SEVERE CORE DAMAGE ACCIDENTS vs. OPERATING YEAR
$f(1/yr)$

<table>
<thead>
<tr>
<th>yr</th>
<th>75</th>
<th>76</th>
<th>77</th>
<th>78</th>
<th>79</th>
<th>80</th>
<th>81</th>
<th>82</th>
<th>83</th>
</tr>
</thead>
<tbody>
<tr>
<td>f(1/yr)</td>
<td>2×10^{-4}</td>
<td>1×10^{-4}</td>
<td>5×10^{-5}</td>
<td>2×10^{-5}</td>
<td>1×10^{-5}</td>
<td>5×10^{-6}</td>
<td>2×10^{-6}</td>
<td>1×10^{-6}</td>
<td>5×10^{-7}</td>
</tr>
</tbody>
</table>
### German Precursor Study

#### Trend of the Frequency of Potential Severe Core Damage Accidents

<table>
<thead>
<tr>
<th>Year</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>1975–1983</td>
<td>$4.7 \times 10^{-5}$/yr</td>
</tr>
<tr>
<td>1975–1979</td>
<td>$8.4 \times 10^{-5}$/yr</td>
</tr>
<tr>
<td>1980–1983</td>
<td>$1.1 \times 10^{-5}$/yr</td>
</tr>
</tbody>
</table>

### Contributions to the Frequency of Potential Severe Core Damage Accidents (1/yr)

<table>
<thead>
<tr>
<th>Types of Initiating Events</th>
<th>German Precursor Study</th>
<th>German Risk Study</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of main feedwater</td>
<td>$2.1 \times 10^{-5}$</td>
<td>$3 \times 10^{-6}$</td>
</tr>
<tr>
<td>Loss of preferred power</td>
<td>$1.6 \times 10^{-5}$</td>
<td>$1.3 \times 10^{-6}$</td>
</tr>
<tr>
<td>Loss of main heat sink without loss of main feedwater</td>
<td>$1 \times 10^{-8}$</td>
<td>$3 \times 10^{-6}$</td>
</tr>
<tr>
<td>Small leak in pressurizer during loss of preferred power</td>
<td>$8 \times 10^{-7}$</td>
<td>$7 \times 10^{-6}$</td>
</tr>
<tr>
<td>Small leak in pressurizer during other transients</td>
<td>$2.4 \times 10^{-6}$</td>
<td>$2 \times 10^{-6}$</td>
</tr>
<tr>
<td>Small leak in pressurizer due to spurious opening of pressurizer valves</td>
<td>$1.5 \times 10^{-6}$</td>
<td>-</td>
</tr>
<tr>
<td>Small leak in a reactor coolant loop</td>
<td>-</td>
<td>$5.7 \times 10^{-6}$</td>
</tr>
<tr>
<td>ATWS</td>
<td>-</td>
<td>$1 \times 10^{-6}$</td>
</tr>
</tbody>
</table>

**Final Results (October 1985)**
INTRODUCTION

This study has been prepared by the GRS by contract of the Federal Ministry of Interior. The purpose of the study is to show how the application of system-analytic tools and especially of probabilistic methods on the Licensee Event Reports (LERs) and on other operating experience can support

- a deeper understanding of the safety-related importance of the events reported in reactor operation,
- the identification of possible weak points,
- further conclusions to be drawn from the events.

Additionally, the study aimed at a comparison of its results for the severe core damage frequency with those of the German Risk Study as far as this is possible and useful.

The decision to perform such a study was influenced especially by the U.S. Accident Sequence Precursor (ASP) program (1, 2) which had to identify and evaluate precursors to potential severe core damage accidents on the basis of operating experience as documented in the LERs.

In the ASP-study plant differences were taken into account on a limited basis, i.e. by different specializations of the generic event trees. No differences in the reliability data were considered. However, many comments on the ASP-study exist so that precursor studies should be performed on a plant-specific basis using plant-specific data (3).

The German Precursor Study is a plant-specific study. The reference plant is Biblis NPP with its very similar Units A and B, whereby the latter was also the reference plant for the German Risk Study (4, 5). The reasons for this choice were the following:

- The technical lay-out of both Biblis units is very similar especially for the safety systems. The operating experience for these systems is therefore generally transferable.
- Both units together comprise the longest operating experience of all German NPPs.
- For the Biblis NPP detailed informations about the operating experience were available at GRS, both, with respect to initiating events and with respect to failures in the safety systems. The latter was gained by a very detailed reliability data collection in Biblis, Unit B (6, 7), which was also performed by GRS.
- The event trees and fault trees of the German Risk Study could be used.
- The Biblis NPP is among all plants with similar operating experience the most representative plant for the German PWRs, which are now operating or are to be licensed.
- The results of the evaluations of the German Precursor Study can be compared with the results of the reliability analyses of the German Risk Study.

METHODOLOGY AND DATA BASE COMPARED WITH THE ASP-STUDY

In the Federal Republic of Germany there are currently 7 PWRs and 6 BWRs in operation, the sum of the reactor operations add up to 62 years for the PWRs and 32 years for the BWRs. This corresponds to about 20 % of the U.S.-operating experience between 1969 and 1979, which was investigated in the ASP-study (1). Currently, there are about 1500 LERs recorded in the Federal Republic of Germany.

Total failures of safety systems have been observed only in very few cases. As a consequence the probabilities of total system failures cannot be obtained by applying the same methodology as in the ASP-study. On the other hand, partial failures of the safety systems have not to be reported in the LERs in all cases. Unavailabilities of partial systems and especially train unavailabilities can therefore generally not be derived from LERs, with the exception of Diesel-generator failures and control rod failures.

Initiating events which contributed significantly or at least notably to the assessed core melt frequency in the German Risk Study were:

- Small leak in a reactor coolant loop
- Loss of preferred power (emergency power case)
Other transients, which lead to a demand of the pressurizer relief valves.

Loss of main feedwater

A "small leak" in a reactor coolant loop or via a stuck open pressurizer relief valve has not been observed within the German operating experience with PWR plants. On the other hand, the reporting criteria do not require to report the demands of the pressurizer relief valves and the other above mentioned transients in any case. Therefore, an evaluation of the frequencies of these transients was not possible on the basis of the LERs.

The way to overcome this difficulty was to use the additional operating experience of the Biblis NPP in the following way:

- Based on detailed information about initiating events during the time period from the beginning of commercial operation (February 1975 for Unit A and January 1977 for Unit B) until the end of 1983, plant-specific frequencies of the initiating events were assessed.
- Based on the reliability data collection of Biblis B (§ 2), plant-specific mean unavailabilities of the system trains were estimated to calculate plant-specific unavailabilities of system functions.
- Total system failures, multiple failures and potential multiple failures were considered, when plant-specific operating experience exists. An evaluation of total system failures or multiple failures based on the overall German operating experience would inevitably lead to similar critiques as in the ASG-study with respect to the problem of transferability; such an evaluation should not be done in a plant-specific precursor study, but be performed in risk studies.
- Operator errors after occurrence of an initiating event were quantified, when some plant specific operating experience was available.

That means, the German Precursor Study intentionally restricts itself on initiating events, failures within the systems and manual interventions after occurrence of an initiating event, known from the plant-specific experience. This is different to a risk study where events also have to be considered, which have not been observed so far (as a main steam line break etc.).

The initiating events during plant operation were considered and evaluated as if all of them had occurred during full load operation. The same pessimistic minimal requirements for the system functions were used as in the German Risk Study; they were taken from the licensing process.

Manual interventions after occurrence of an initiating event were taken into account in the following way:

- The frequencies of the initiating events and of the event sequences were estimated accounting for rectifying the initiating event and performing manual interventions, respectively. The corresponding probabilities were assessed from the plant-specific field experience.
- Manual interventions, which were possible but not performed in such situations, were not taken into account.

The first method of taking manual interventions into account is the same as the general approach of the ASG-study for the initiating events "loss of main feedwater" and "loss of preferred power". The second method deviates from the ASG-method, where credit was given for such manual interventions by severity factors (1) and recovery classes (2), respectively.

As precursors to potential severe core damage accidents, the following types of events were selected:

- Events, which led as initiators not only to a reactor scram but also to a demand on further safety systems or safety-related systems.
- Events, where
  -- a total loss of a system function or
  -- a multiple failure or a potential multiple failure occurred.

The probability evaluations performed in the German Precursor Study for the different precursors were similar to the ASG-study. Therefore, the fault trees of the German Risk Study were used. Only mean values have been assessed; as in the ASG-study (1) statistical uncertainties were not calculated, but this task has recently been started. Due to the limited data base (16 years of reactor operation for the initiating events; 3.5 years of operating experience for the train unavailabilities) remarkable uncertainty bounds can be expected.

The individual event sequences were evaluated considering both, the frequency of the initiating event and the probabilities of system failures at that time, when the initiating event occurred. Because of the system modifications, which have been introduced throughout the years of operation, the frequencies and probabilities changed. Hence, the results of the German Precursor Study cannot simply be transferred to the present situation.
The trend in the overall frequency per reactor year of events selected as precursor in both units of Biblis NPP is shown in Fig. 1. Fig. 2 shows the trend in the overall frequency per reactor year of potential severe core damage accidents. The main contributions to the severe core damage frequency come from the first years of plant operation; its decrease with increasing operating time is due to numerous system improvements. The mean value of the overall frequency of potential severe core damage accidents is $4.7 \times 10^{-5}$ per reactor year. This result is based on the assumption, that the failure mechanisms of the system trains can be described by constant failure rates. Under the pessimistic assumption of constant failure probabilities per demand the result would increase only by a factor of 2.

The above mentioned results fit into the 90% confidence interval for the core melt frequency which was obtained by the German Risk Study reaching from $1 \times 10^{-5}$ to $3 \times 10^{-4}$ per reactor year, with a mean value of $9 \times 10^{-5}$ per reactor year. One reason for the lower mean value in comparison to the German Risk Study is due to the limited existing operating experience, i.e. the study was restricted to initiating events, system and multiple failures as well as human actions which occurred during the observation period.

The individual contributions to the severe core damage frequency show, however, larger discrepancies (Table 1). In contrary to the German Risk Study there is no contribution to the total result from a "small leak in a reactor coolant loop" or from ATWS, because either the initiating event did not occur or no malfunction of the reactor scram system was observed in the operating experience.

The results for the "loss of preferred power" are in accordance with the results of the German Risk Study. The agreement is satisfactory for the "small leaks in pressurizer". These results were derived from the frequency of demands of the pressurizer relief valves and the probability of failure of the PORVs and the redundant block valves to re-close. It should be noted that for these initiating events larger frequencies were gained than in the German Risk Study. On the other hand significantly lower probabilities of failure of the associated system functions were received.

The assumption of the German Risk Study that each "loss of preferred power" would lead to a demand of pressurizer relief valves has not been supported by the operating experience.
Table 1
CONTRIBUTIONS TO THE FREQUENCY OF POTENTIAL SEVERE CORE DAMAGE ACCIDENTS

<table>
<thead>
<tr>
<th>Initiating Event</th>
<th>German Precursor Study</th>
<th>German Risk Study</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of main feedwater (without small LOCA via pressurizer)</td>
<td>2.0 x 10^{-5}/yr</td>
<td>3 x 10^{-6}/yr</td>
</tr>
<tr>
<td>Loss of preferred power (without small LOCA via pressurizer)</td>
<td>1.5 x 10^{-5}/yr</td>
<td>1.3 x 10^{-5}/yr</td>
</tr>
<tr>
<td>Loss of main heat sink, without loss of main feedwater</td>
<td>1 x 10^{-8}/yr</td>
<td>3 x 10^{-8}/yr</td>
</tr>
<tr>
<td>Small leak in pressurizer during loss of preferred power</td>
<td>9 x 10^{-7}/yr</td>
<td>7 x 10^{-6}/yr</td>
</tr>
<tr>
<td>Small leak in pressurizer during other transients</td>
<td>2.4 x 10^{-6}/yr</td>
<td>2 x 10^{-6}/yr</td>
</tr>
<tr>
<td>Small leak in pressurizer due to spurious opening of pressurizer valves</td>
<td>1.6 x 10^{-6}/yr</td>
<td>-</td>
</tr>
<tr>
<td>Small leak in reactor coolant loop</td>
<td>-</td>
<td>5.7 x 10^{-5}/yr</td>
</tr>
<tr>
<td>ATWS</td>
<td>-</td>
<td>1 x 10^{-6}/yr</td>
</tr>
</tbody>
</table>

During the observed time period a significant improvement of the plant behaviour can be stated. At the beginning of commercial operation the dominant contribution was given by the "loss of main feedwater and main heat sink" due to a actuation of the main steam line break-signal. This initiating event was only observed in the first half time interval (till end of 1978) and can be interpreted as an initial problem, leading to improvements of the actuation devices, of the control of the main steam bypass valves and of the operator manual.

In the second half time period (1980-1983) the most important contributions came from the potential multiple failure of three residual heat removal pumps (in 1983) and from the "loss of preferred power". Meanwhile, the electric power supply of Biblis NPP was improved by the installation of a second independent grid connection to each unit. Therefore, the expected contribution of this initiating event will be much lower now.

The frequency of the opening of the first pressurizer relief valve decreased from 0.9 per reactor year in the first half time interval to 0.5 per reactor year in the second half time interval, the frequency of the opening of both pressurizer relief valves remained constant with 0.25 per reactor year.

A considerable reduction of the contribution of a "small leak in pressurizer" to the frequency of potential severe core damage nearly exclusively results from several improvements of the pressurizer system, especially of the control valves for the pilot valves and block valves.

In comparison with the German Risk Study the operating experience of Biblis NPP has not revealed any new types of initiating events.

Human error has influenced 50 % of the events selected as precursors. These events contribute 67 % to the total result. However, one has to be aware that the present situation of documentation of operating experience is not sufficient for cause-oriented evaluation of human errors.

OUTLOOK

For proving and supporting the plant-specific results of the German Precursor Study as reported in this paper, the transferability of LERs from all other German nuclear power plants to Biblis NPP will be checked. This will be done in two steps, answering the following questions:
Have additional types of initiating events occurred at other plants? How are these events transferable to Biblis NPP?

Have additional total failures of systems and multiple failures, respectively, occurred in other plants? How are these failures transferable to Biblis NPP?

The corresponding investigations have already been started.

REFERENCES


3. "ACRS Report on the Accident Sequence Precursor Study and the Use of Operational Experience", from J. Ebersole. (ACRS) to W. Dircks, dated May 18, 1983

4. GRS: Deutsche Risikostudie Kernkraftwerke, Hauptband und Fachbände, Verlag TUV Rheinland, 1979


we tried to estimate the major influencing parameters for a large variety of types of components. During this collection all safety relevant systems have been observed for about four years. This covers about 17,000 components, which consist of about 40,000 items.

Evaluation of Influencing Parameters

In this paper we concentrate on our evaluations on valves which are with 7,476 components the largest population. In Table 1 a distribution of the different types of valves and their actuation is shown. For each valve up to 60 parameters are stored in our data base describing engineering and operational characteristics. The failure data are based on the maintenance information system, which has been upgraded by additional codification and continuous control of the data. For the valves 3,148 maintenance orders have been filled in during the observation time, 1,170 of which were written in request to repair a failure or a deficiency, the rest of 1,978 orders dealt with preventive maintenance.

The evaluation has started with an analysis of the qualitative failure characteristics. Especially the mode of failure, the failure detection, the immediate failure effects, the effect during repair and the type of repair has been analysed. This has been done to develop an understanding of the overall failure behavior compared to the behavior of the special type of equipment. This knowledge has been very useful for the selection and discussion of parameters the influence of which had to be analysed.

For the evaluation of the influencing parameters from the available parameters 17 have been choosen, they are listed in Table 2. Only parameters for which a contribution was expected are included.

For each parameter subpopulations had to be set up for the statistical treatment. The subdivision was done with respect
to the number of failures in each subpopulation to get statistically significant answers. The definition of subpopulations creates sometimes problems, in this cases we used expert judgement for the decision.

For the evaluation of the data a computer program was utilized, which carried out the following tasks.

- Selection of a component or item population from the data base according to preselected criteria
- Selection of failure reports with preselected criteria for each component
- Estimation of operating or observation hours for each component
- Subpopulation formation for each parameter
- Calculation of failure rates for each subpopulation
- Calculation of the statistical significance for subpopulation rates
- Print out of the results and a complete list of data used during the processing by request.
- Plotting of distributions

The program is controlled by a menu where the parameters, functions, selection criteria can be chosen. The chi-squared test is used to estimate if a parameter has statistically significant influence.

Discussion of Results

In figure 1 and table 3 the variability of results for the failure modes "Doesn't operate on request" and "external leakage" for the different types and actuation modes of the valves are shown as mean values. As can be seen there is a quite strong dependency on this two parameters even for the mean values of those classes. But more interesting is the behavior of the same type which is shown for the failure mode "Doesn't operate in figure 2, 3 and 4 and for external leakage" in figure 5, 6 and 7. In these figures only those parameters are shown which have a significant influence. This means these are the influencing parameters. For the other parameters which are listed in table 2 an influence could not be determined. The results are depending on the parameters are quite different. Taking the example "gate valve" the smallest difference is calculated for the disk type with a factor of 1.6 and the highest for system and operating pressure with a factor of 53. The statistical evaluation of the influences in most cases have been done separately parameter by parameter, but there are relations between the parameters. By an engineering analysis of the dependencies and the failure types we figured out the most relevant influences, which should by used for a data transfer. Mostly the combination of two and more influences have the most severe influence. But nevertheless sometimes additional factors, which were not taken in consideration during the collection play an important role. For gate valves this has been the differential pressure during operation, which had not been taken in consideration at the beginning, because these data are not available in the plant documentation and therefore are difficult to obtain. This is the explanation for the highest calculated failure rate.

The overall experience gained during the evaluation of the results is, that because of the limited number of similar components and equipment with similar operating conditions there is still a greater effort of engineering judgement necessary for the evaluation of results and their transfer to other projects.
Importance to the credibility of PSA-results

For some PSA-projects we have evaluated the data base taking into consideration the uncertainties of failure rates. For some types we come out with uncertainty ranges of the failure rate near to two orders of magnitude. This means there is a considerable influence on the results of the analysis, when safety systems have four completely separated trains like in the FRG.

PSA-results will only be used for decisions, if there is confidence that the prediction will match the reality, bearing in mind that there is a certain degree of uncertainty. This uncertainty has to be kept low. As shown before the influences on the failure behavior must be known and used for the setting up of data sets for analysis to get more credibility for probabilistic analyses.

Besides the figures the better knowledge on the failure behavior can help in the choose of components, in the assessment if components have reached their intended reliabilities, for changing operation methods, etc.

Conclusion

It was demonstrated, that there are a number of parameters which influence the failure behavior in different ways. Especially for highly redundant systems this affects the PSA-results in a high grade. Therefore there is a need to use such specified data to reduce the uncertainties of the results and to improve the credibility of PSA for decision making of plant management.

**TABLE 1: LIST OF VALVE SUBPOPULATIONS**

<table>
<thead>
<tr>
<th>VALVETYPE</th>
<th>ACTUATION</th>
<th>MODE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>REMOTE</td>
<td>MANUELL</td>
</tr>
<tr>
<td>STOP GATE VALVE</td>
<td>106</td>
<td>355</td>
</tr>
<tr>
<td>STOP DISK VALVE</td>
<td>344</td>
<td>3,786</td>
</tr>
<tr>
<td>STOP BUTTERFLY VALVE</td>
<td>55</td>
<td>204</td>
</tr>
<tr>
<td>STOP COCK VALVE</td>
<td>-</td>
<td>342</td>
</tr>
<tr>
<td>CONTROLL VALVE, DISK</td>
<td>124</td>
<td>51</td>
</tr>
<tr>
<td>CONTROLL VALVE, BUTTERFLY</td>
<td>169</td>
<td>41</td>
</tr>
<tr>
<td>THROTTLE DISK VALVE</td>
<td>37</td>
<td>104</td>
</tr>
<tr>
<td>THROTTLE BUTTERFLY VALVE</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>SAFETY VALVES</td>
<td>-</td>
<td>413</td>
</tr>
<tr>
<td>FIRE FLAP</td>
<td>196</td>
<td>2</td>
</tr>
<tr>
<td>CHECK VALVE, DISK TYPE</td>
<td>484</td>
<td>-</td>
</tr>
<tr>
<td>CHECK VALVE, SWING TYPE</td>
<td>216</td>
<td>-</td>
</tr>
<tr>
<td>MULTI-WAY GATE VALVE</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>MULTI-WAY DISK VALVE</td>
<td>311</td>
<td>83</td>
</tr>
<tr>
<td>MULTI-WAY COCK</td>
<td>-</td>
<td>32</td>
</tr>
<tr>
<td>SEPARATION TRAP</td>
<td>-</td>
<td>20</td>
</tr>
<tr>
<td>OTHER VALVE</td>
<td>-</td>
<td>2</td>
</tr>
</tbody>
</table>
### Table 2: List of Analyzed Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacture Type</td>
<td>Operating Pressure</td>
</tr>
<tr>
<td>Manufacture Type</td>
<td>Operating Temperature</td>
</tr>
<tr>
<td>Mode of Operation</td>
<td>Media Handled</td>
</tr>
<tr>
<td>Kind of Power Rating</td>
<td>Nominal Size</td>
</tr>
<tr>
<td>Shaft Sealing Type</td>
<td>Actuation Type</td>
</tr>
<tr>
<td>Vibration</td>
<td>Disk Type</td>
</tr>
<tr>
<td>Nominal Power</td>
<td>Demand Frequency</td>
</tr>
<tr>
<td>Nominal Torque</td>
<td>Revolutions per Shift Way</td>
</tr>
<tr>
<td>Drive Rotational Speed</td>
<td></td>
</tr>
</tbody>
</table>

### Table 3: Failure Rates of Valve Subpopulations, Mean Values ($x \times 10^{-6}$ /h)

Failure Mode "Doesn't Operate"

<table>
<thead>
<tr>
<th>Valve Type</th>
<th>Actuation</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop Gate Valve</td>
<td>28.6</td>
<td>1.7</td>
</tr>
<tr>
<td>Stop Disk Valve</td>
<td>14.1</td>
<td>0.5</td>
</tr>
<tr>
<td>Stop Butterfly Valve</td>
<td>24</td>
<td>3.2</td>
</tr>
<tr>
<td>Stop Cock Valve</td>
<td>-</td>
<td>0.5</td>
</tr>
<tr>
<td>Control Valve Disk</td>
<td>33.5</td>
<td>6.5</td>
</tr>
<tr>
<td>Control Valve Butterfly</td>
<td>28.5</td>
<td>0.5</td>
</tr>
<tr>
<td>Throttle Disk Valve</td>
<td>-</td>
<td>2.5</td>
</tr>
<tr>
<td>Throttle Butterfly Valve</td>
<td>168</td>
<td>-</td>
</tr>
<tr>
<td>Safety Valves</td>
<td>3.8</td>
<td>0.3</td>
</tr>
<tr>
<td>Fire Flap</td>
<td>15.3</td>
<td>-</td>
</tr>
<tr>
<td>Check Valve, Disk Type</td>
<td>31.5</td>
<td>0.7</td>
</tr>
<tr>
<td>Valve, Swing Type</td>
<td>-</td>
<td>0.4</td>
</tr>
<tr>
<td>Multi-Way Gate Valve</td>
<td>3.8</td>
<td>-</td>
</tr>
<tr>
<td>Multi-Way Disk Valve</td>
<td>10.7</td>
<td>3.3</td>
</tr>
<tr>
<td>Separation Trap</td>
<td>-</td>
<td>2.1</td>
</tr>
</tbody>
</table>
### Table 4: Failure Rates of Valve Subpopulations, Mean Values (x 10^{-6} 1/H)

<table>
<thead>
<tr>
<th>Valvetype</th>
<th>Actuation Mode</th>
<th>Manuell</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop Gate Valve</td>
<td>23</td>
<td>3,1</td>
</tr>
<tr>
<td>Stop Disk Valve</td>
<td>4,1</td>
<td>2,0</td>
</tr>
<tr>
<td>Stop Butterfly Valve</td>
<td>6,9</td>
<td>0,4</td>
</tr>
<tr>
<td>Stop Cock Valve</td>
<td>-</td>
<td>0,2</td>
</tr>
<tr>
<td>Controll Valve, Disk</td>
<td>14,0</td>
<td>1,4</td>
</tr>
<tr>
<td>Controll Valve Butterfly</td>
<td>0,3</td>
<td>-</td>
</tr>
<tr>
<td>Throttle Disk Valve</td>
<td>-</td>
<td>0,8</td>
</tr>
<tr>
<td>Safety Valves</td>
<td>-</td>
<td>4,9</td>
</tr>
<tr>
<td>Fire Flap</td>
<td>0,2</td>
<td>-</td>
</tr>
<tr>
<td>Check Valve, Disk Type</td>
<td>-</td>
<td>3,7</td>
</tr>
<tr>
<td>Check Valve, Swing Type</td>
<td>-</td>
<td>2,5</td>
</tr>
<tr>
<td>Multi-Way Disk Valve</td>
<td>15,6</td>
<td>1,8</td>
</tr>
<tr>
<td>Separation Trap</td>
<td>-</td>
<td>37,8</td>
</tr>
</tbody>
</table>
OBJECTIVES AND METHODS OF RELIABILITY DATA COLLECTION
AND ANALYSIS AT LOVIISA POWER PLANT

J.K. Vaurio
IMATRAN VOIMA OY
07900 Loviisa, Finland

INTRODUCTION

The reliability data collection and analysis system under development for the Loviisa Nuclear Power Plant has two main goals:

1) Obtain plant specific data and parameters for probabilistic safety assessment (PSA) project underway, and

2) Establish on-line data collection and analysis system for the future.

The latter system allows updating of parameters for a living PSA, and facilitates trend studies and feedback from experience to optimize maintenance planning, spare parts inventory, technical specifications and limiting conditions for operation. This paper is focused on the details of a PSA data system because plans for the on-line systems are less advanced. Nevertheless, the PSA data system is designed to be part of the on-line system eventually. Objectives set for the PSA data system are discussed together with techniques used to accomplish the objectives.

The first objective for the data collection effort is to

- obtain parameters for comprehensive component models.

Generic data sources usually provide most common parameters such as failure rates and probabilities of failure per demand. Not enough attention has been paid to recording failure entering, detection and repair mechanisms to allow correct estimation of all parameters needed for proper modeling of the time dependent unavailability of periodically tested standby safety components. Thus, a detailed plant specific data collection system was established. This decision is supported by the second objective

- avoid bias and excessive uncertainty of generic data

This is particularly important for a plant, like Loviisa, that has both eastern and western technology throughout the plant. No generic data bank is applicable as such. Furthermore, generic data has been collected from many different plants, and data variability tends to exceed that on any single plant that has operating experience data.

Of course, when plant data is collected there are always some components with very little or no failures. When this fact is combined with the third objective to

- use realistic non-zero failure rates for all components,

it is natural to select an estimation method that allows to use information from other "similar" components when data is scarce. The Bayes method satisfies this condition. The fourth objective

- minimize subjectivity in parameter estimation,

forces us to seek empirical basis for prior distributions. When combined with objectives 1 and 2, it leads to maximum use of plant specific data. It is necessary, though, to allow expansion of the
class of "similar" components until sufficient data is available for estimation.

The fifth objective requires us to have the possibility for

- convenient sensitivity studies, using alternative prior assumptions.

Selecting families of conjugate prior distributions allows such sensitivity studies performed by simple adjustments of distribution parameters. Thus, gamma prior distributions are used for Poisson observations (number of failures in a specified time), and beta distribution for binomial observations (number of errors in a specified number of attempts).

Finally, a special method has been developed for parameter estimation such that it is robust for small samples and consistent with classical fiducial confidence levels in case of no prior information (or identical observations). It is also asymptotically unbiased as the sample size or observation time increases.

The role and objectives discussed above are illustrated in Fig. 1.

The resulting posterior mean values can be used in "best estimate" or "point value" calculations. However, since distributions become available, they can be used in uncertainty analysis, Monte Carlo type procedures.

Since beginning of operation, 1977 for Loviisa 1 and 1980 for Loviisa 2, significant learning has taken place, reducing failure rates on certain components. Thus, some trend analysis is needed to be able to use current estimate values. Learning models have been developed to carry out trend analysis.

DATA COLLECTION

Two important component characteristics used in current risk assessments are

(1) Failure rates for components that cause initiating events i.e. their failures activate one or more safety functions;

(2) Unavailabilities (fractional dead times) for components needed after initiating events to accomplish a safety function.

The unavailabilities used in base calculations are time-averaged values. Time dependent analysis will be performed for important failure combinations to verify that scheduling of testing etc. doesn't change results excessively. An advanced version of the well known FRANTI code1 will be used in such calculations, and Fig. 2 illustrates a typical unavailability curve of a standby component2. While failure rates are relatively easy to estimate from observed numbers of failures, unavailabilities depend on several parameters due to many possibilities of failures entering and being detected and repaired. A special data collection form has been developed to gather all relevant information about events. Items are listed in Table I.

First, each component belongs to one of the three categories: (A) Normally standby, (B) normally operating, or (C) alternating standby and operation. Any unavailability of a component falls into one of the following classes

Class K: Fatal hardware failures; unavailability begins when the failure enters and continues through repair.

Class L: Incipient hardware faults that need to be fixed but the component is unavailable only during the repair (unscheduled maintenance).
Class M: The unavailability is due to scheduled periodic maintenance or testing taking a component out of service for some time.

Class H: The unavailability is due to human errors made in a periodic maintenance, test, calibration or restoration thereafter.

In terms of modeling, events in classes K and L enter due to a failure rate that is usually different in standby and operating modes. Events of class N enter with a certain error probability per maintenance action or attempt. Class M events are fixed periods of unavailability at fixed times.

Failure detection method (item 11) and likely failure entry time (item 12) are extremely important for calculating the unavailability time of each event from information in item 15. For example, the unavailability time for class L events is \( t_4 - t_3 \) for both standby and operating components, while \( t_4 - t_1 \) is valid for all class K failures that are detected immediately due to alarms or other symptoms. In addition to times in item 15, periodic testing information from item 7 is needed for standby components for failures detected or entering due to testing.

Equations for all possible combinations of answers to items in Table I have been developed, to obtain unavailability parameters needed in basic quantification and in time dependent calculations.

One may notice that "cause" as an item is not listed on Table I. Causes are recorded in narrative form only, because of uncertainties and subjectivity in interpretation. Furthermore, several causes are often involved for important events, and for many others it is not possible to identify a definite cause. Answers to items 3 (Actions taken), 12 (Failure entry) and 6 (Failure mode) often discover the main characteristics of the cause.

<table>
<thead>
<tr>
<th>Table I - Data Items Relevant to PSA Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Event/Work report identification</td>
</tr>
<tr>
<td>2. Component/System/Location identification</td>
</tr>
<tr>
<td>3. Actions taken (repair, replacement, parts etc.)</td>
</tr>
<tr>
<td>4. Component category: A. Standby, B. Operating, C. Alternating</td>
</tr>
<tr>
<td>5. Unavailability class: K. Fatal, Failure, L. Fault (repair)</td>
</tr>
<tr>
<td>6. Failure mode (coded list)</td>
</tr>
<tr>
<td>7. Periodic test interval and duration</td>
</tr>
<tr>
<td>8. Unavailability impact on system</td>
</tr>
<tr>
<td>9. Other events due to the same cause</td>
</tr>
<tr>
<td>10. Event impact on plant production</td>
</tr>
<tr>
<td>11. Event detection method</td>
</tr>
<tr>
<td>12. Failure/Fault entry (likely)</td>
</tr>
<tr>
<td>13. Design error</td>
</tr>
<tr>
<td>14. Design criteria changed</td>
</tr>
<tr>
<td>15. Times:</td>
</tr>
<tr>
<td>a. Previous test or maintenance ( t_0 )</td>
</tr>
<tr>
<td>b. Failure/Fault detection ( t_1 )</td>
</tr>
<tr>
<td>c. Repair permit ( t_2 )</td>
</tr>
<tr>
<td>d. Repair beginning ( t_3 )</td>
</tr>
<tr>
<td>e. Repair completed ( t_4 )</td>
</tr>
<tr>
<td>f. Return to use ( t_5 )</td>
</tr>
</tbody>
</table>
ESTIMATION OF PARAMETERS

The failure rate, $\lambda$, and the unavailability per demand, $q$, are the most important characteristics needed for reliability and availability analysis. Test intervals are fixed constants and need no estimation. Average repair times are also relatively accurate. If needed, repair rate can be estimated using the same formalism as available for failure rates, just by replacing observed times to failure by observed repair times. Thus, only estimation of $\lambda$ and $q$ is discussed in this section.

According to Fig. 1 the estimation method selected is a Bayesian technique with empirically determined prior distributions for $\lambda$ and $q$. Values to be used in risk calculations are based on individual posterior distributions of each component: posterior mean values are used in the base case calculations, and the whole posterior distributions are used in uncertainty calculations.

The prior distribution of a pump, for example, is determined from a sample of $k$ identical pumps that are parallel or redundant in a system. In case few or no failures have taken place in those pumps, the sample can be increased to include other similar pumps with the same manufacturer and roughly the same characteristics and use. Expansion of the sample usually leads to widening of the prior distribution, but it guarantees realistic non-zero failure rates, is consistent with plant specific spectrum of manufacturers and use, with minimal dependence on generic (perhaps atypical) worldwide data.

The estimation of failure rates involves $k$ components (or groups of components) with observation times $T_i$ and numbers of failures $K_i$, $i=1,2,...,k$. The observable $K_i$ has a Poisson probability distribution with mean and variance $\lambda_i T_i$. The purpose is to estimate the (posterior) probability densities of individual failure rates $\lambda_i$. The prior density of all $\lambda_i$ ($i=1,2,...,k$) is assumed to be a gamma distribution, a conjugate for a Poisson likelihood. The parameters of such a prior are determined by a modified moment matching method. Equations of the estimation of the prior mean value $\mu$ and variance $V$ are listed on Table II.

The basic new feature in these equations are the bias terms $s_1$ and $s_2$ that bring about many good characteristics:

1. A realistic solution for a gamma prior exists for any values of $k>1$, as long as there are any failures (at least one $K_i>0$) even for small $k$ and when data are closely clustered (small $V$); such cases have been problematic to many earlier methods.

2. With identical data ($V=0$, which is quite possible for small samples) the "optimistic" case yields a posterior probability distribution that is consistent with assuming identical components (pooled data) and obtaining classical fiducial lower confidence levels. This again is consistent with assuming a Jaynes-Jeffreys prior $-1/\lambda$.

3. With identical data ($V=0$) the "conservative" case yields a posterior distribution consistent with pooled data and classical fiducial upper confidence levels. This then is consistent with assuming a uniform prior for the pooled data.

4. Asymptotically with increasing $k$ (and $T$) the relative influence of the bias terms is diminishing.

5. The weights $w_i$ defined in Table II are optimal in the sense that they approximately minimize the expected mean square error (variance) of the estimate $\hat{\mu}$. This weighting reduces the influence of components with small $T_i$, and equalizes the impact of components with very large $T_i$.

6. It can be shown that the posterior mean values can also be presented as Steins estimators.
Table II - Equations for Prior Moment Matching

\[
N = \bar{m} + s_1
\]  \hspace{1cm} (1)

\[
V = \bar{v} + \frac{s_2}{T^*}
\]  \hspace{1cm} (2)

where

\[
\bar{m} = \sum_{i=1}^{k} w_i \frac{K_i}{T_i}
\]  \hspace{1cm} (3)

\[
\bar{v} = \frac{k}{k-1} \sum_{i=1}^{k} u_i \left( \frac{K_i}{T_i} - \bar{m} \right)^2
\]  \hspace{1cm} (4)

\[
s_2 = \left( 1 + \frac{\bar{v}}{\bar{m}} T^* \right) s_1
\]  \hspace{1cm} (5)

\[
u_i = \begin{cases} 0, & \text{for "optimistic" version} \\ \frac{1}{T_i}, & \text{for "conservative" version} \end{cases}
\]  \hspace{1cm} (6)

\[
u_i = u_i / \sum_{j=1}^{k} u_j
\]  \hspace{1cm} (7)

\[
u_i = \frac{T_i}{(T_i + N/V)}
\]  \hspace{1cm} (8)

\[
T^* = T - \max(T_i)
\]  \hspace{1cm} (9)

\[
T = \sum_{i=1}^{k} T_i
\]  \hspace{1cm} (10)

\[
\hat{\lambda}_i = \frac{1}{B_i} \frac{K_i}{T_i} + B_i \bar{m}.
\]

where the shrinking factors are

\[
B_i = 1 - u_i + N/(N + V T_i).
\]

These minimize the mean square errors of \( \hat{\lambda}_i \)'s.

Further details can be found in Ref. 3.

For estimation of \( q_i \), the probability of failure of component \( i \) per demand, the observables \( K_i \) are binormal variables with mean value \( q_i N_i \). The conjugate prior in this case is a beta distribution. The equations of Table II are still approximately valid for determining moments for the prior if \( T_i \) is replaced with \( N_i \), the number of demands or attempts observed\(^8\).

RELIABILITY TRENDS AND LEARNING MODELS

During ten years of Lovisa I reactor operation many failure rates have significantly reduced. This has been demonstrated by separate studies on certain pumps, valves and diesel generators. A study\(^5\) on makeup pumps and high pressure ECC pumps has indicated that much of the unavailability is due to unscheduled maintenance of developing flaws rather than fatal failures, and most faults are caused by periodic testing startups rather than randomly in time. Such results lead to a recommendation to eliminate testing or extend test intervals. For diesel generators, test intervals have been extended for similar reasons, and test procedure changed to reduce defects developing due to cold startup shocks on diesels.

For a general trend analysis in a PSA one can assume a general form \( n = A T^B \) for the expected number of failures, \( n \), as a function of the total time on duty (or number of tests), \( T \). For \( B > 1 \) the model describes increasing failure rates due to ageing. Several formulations have been derived in Ref. 6 to estimate parameters \( A \) and \( B \) of such a Weibull model. The method is based on plotting the
Objective 1: Obtain parameters for comprehensive component models

Decision: Use plant specific data

Consequence: No failure data for some components

Objective 2: Avoid bias and excessive uncertainty of generic data

Decision: Use empirical Bayes method, with priors based on plant data

Objective 3: Use realistic non-zero failure rates for all components

Objective 4: Minimize subjectivity in parameter estimation

Decision: Use parametric conjugate prior distributions

Objective 5: Convenient sensitivity studies using alternative prior assumptions

Decision: Use special robust estimation of prior distribution parameters

Objective 6: Use estimation consistent with classical fiducial confidence levels (in case of no prior information)

Fig. 1 - Selecting Methods Based on Objectives

CONCLUSION

The goals and objectives of the reliability data collection efforts at Lorni nuclear power plant have been described. They have led to a logical sequence of applying robust empirical Bayesian framework estimating parameters through a failure entry detection and exit mechanism. A multiplicity of failure entry detection and quantification. Historical data collection should be completely accounted for due to either learning or applying. Some models are being developed and tested for observation verification.
ACKNOWLEDGEMENTS

The author wishes to thank Mr. K.Jänkkila and Mr. U.Lindén of IYO for their assistance in developing many details of the data collection system and related computer programs.

REFERENCES


Merging reliability modelling and operating experience assessment

H.W. Kalfsbeek

Commission of the European Communities,
Joint Research Centre, Ispra Establishment,
Ispra (VA) Italy

Basic aspects

Learning from operating experience for maintaining or improving safety and reliability.

Reliability study of safety functions (systems) tuned as much as possible to observed human and equipment performance, also including non-plant specific experience.

Present availability of
- Advanced modelling techniques and analysis tools
- Readily accessible data banks on operating experience: Incidents/events and equipment performance.
BASIC ELEMENTS

1) Advanced - Easy to use - Reliability analysis tools allowing intense interaction with the analyst
   - CAFTS: Expert system for fault tree construction and analysis. Fault tree linking (event trees)
   - System response analyser (SRA): Time dependent system analysis.

2) Data banks merging broad NPP operating experience - different countries, reactor technologies, operating practices - as compiled in the ERDS
   - AORS: Incident data bank covering 800 years of reactor operation
   - CEDB: Equipment performance covering 22000 component years (pilot stage).
<table>
<thead>
<tr>
<th>CEDB COMPONENT FAMILY</th>
<th># OF COMPONENTS</th>
<th># OF FAILURES</th>
<th>EXPERIENCE COMP. YEARS</th>
<th># OF FAILED COMP.</th>
<th>NOTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>VALVE ACTUATOR</td>
<td>1170</td>
<td>339</td>
<td>5180</td>
<td>203</td>
<td></td>
</tr>
<tr>
<td>BATTERY</td>
<td>35</td>
<td>16</td>
<td>415</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>CIRCUIT BREAKER</td>
<td>247</td>
<td>44</td>
<td>950</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>CLUTCH</td>
<td>2</td>
<td>13</td>
<td>10</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>COMPRESSOR</td>
<td>25</td>
<td>126</td>
<td>405</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>ELECTRIC MOTOR</td>
<td>424</td>
<td>130</td>
<td>1885</td>
<td>101</td>
<td></td>
</tr>
<tr>
<td>INTERNAL COMBUSTION ENGINE</td>
<td>42</td>
<td>140</td>
<td>50</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>HEAT EXCHANGER</td>
<td>93</td>
<td>97</td>
<td>415</td>
<td>43</td>
<td></td>
</tr>
<tr>
<td>FILTER</td>
<td>30</td>
<td>125</td>
<td>135</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>ELECTRICAL GENERATOR</td>
<td>30</td>
<td>20</td>
<td>120</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>PUMP</td>
<td>400</td>
<td>1051</td>
<td>1790</td>
<td>194</td>
<td></td>
</tr>
<tr>
<td>RECTIFIER</td>
<td>27</td>
<td>11</td>
<td>105</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>SAFETY AND RELIEF VALVE</td>
<td>263</td>
<td>318</td>
<td>1130</td>
<td>455</td>
<td></td>
</tr>
<tr>
<td>STEAM GENERATOR</td>
<td>20</td>
<td>74</td>
<td>80</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Switchgear</td>
<td>29</td>
<td>3</td>
<td>110</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>TANK</td>
<td>98</td>
<td>64</td>
<td>480</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>Transformer</td>
<td>20</td>
<td>33</td>
<td>80</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>TURBINE</td>
<td>22</td>
<td>82</td>
<td>90</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>VALVE</td>
<td>2226</td>
<td>1110</td>
<td>9620</td>
<td>633</td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>5173</strong></td>
<td><strong>3766</strong></td>
<td><strong>22470</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
TABLE 5 - Relevant event sequences: AFS emergency operation

<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>78.01.25</td>
<td>Low level in two steam generators, reactor trip, failure to start of turbine driven AFS pump due to closed trip/throttle valve. Valve manually reopened. AFS configuration manually adjusted after 3 hours into the transient.</td>
</tr>
<tr>
<td>78.04.18</td>
<td>Steam generator high level, main feedwater pumps trip, AFS start, low level condensate storage tank. Manual interrupt of AFS to refill storage tank.</td>
</tr>
<tr>
<td>78.12.20</td>
<td>Main feedwater pump trip, no AFS flow to one steam generator due to control valve failure, manual adjustment of AFS configuration to mitigate. Control valve operator repaired one hour into the transient.</td>
</tr>
<tr>
<td>79.07.16</td>
<td>Main feedwater regulator valve failure, no AFS flow to one steam generator due to control valve failure to open. Manual adjustment of AFS configuration.</td>
</tr>
<tr>
<td>79.07.19</td>
<td>Main feedwater controller failure, turbine driven AFS pump trip on overspeed, AFS flow established with electric AFS pumps.</td>
</tr>
<tr>
<td>79.12.30</td>
<td>Reactor trip, low level steam generator, turbine driven AFS pump trip on overspeed, AFS flow established with electric AFS pump.</td>
</tr>
<tr>
<td>80.04.07</td>
<td>Loss of offsite power, degraded AFS flow due to cavitation. Ventiing of AFS pumps train by train during the transient. Cavitation caused by wrong suction design of AFS pumps.</td>
</tr>
<tr>
<td>80.05.06</td>
<td>Loss of feedwater, safety injection, low level steam generator, AFS pump trip on overspeed, flow established by adjusting AFS configuration.</td>
</tr>
<tr>
<td>81.07.22</td>
<td>Spurious main steam isolation valve closure, high steam flow and low pressure on the remaining steam generators, safety injection, failure to start of turbine driven AFS pump. Faulty trip of AFS functioning by the operator.</td>
</tr>
<tr>
<td>84.02.09</td>
<td>Loss of feedwater, low level steam generator, AFS pump trip on overspeed, safety valve fail to close after opening.</td>
</tr>
<tr>
<td>84.03.02</td>
<td>Inadvertent closure main steam isolation valve, reactor trip, high pressure steam generator, safety valve stuck, steam generator boil dry, safety valve closed, no AFS flow because of previously closed AFS valve. Valve manually opened, AFS flow restored.</td>
</tr>
</tbody>
</table>
ABNORMAL OCCURRENCES REPORTING SYSTEM (AORS)

GENERAL CHARACTERISTICS

1. Coded information and free texts
2. Sources of information are national reporting systems on safety related events
3. Event sequence coding: linked occurrences
4. QA programme: checks and incorporation of additional information where available

CODING COMPATIBILITY

UNIT IDENTIFICATION: IAEA
UNIT TYPE: IAEA
EVENT CATEGORIES: NEA-NEA/IAEA
SYSTEMS: ERBD (CEDB, DUSR)
COMPONENTS: USNRC LEA

DEVELOPMENT STEPS AORS

1980: Acquisition of sources: NNC, SKI, CEA, EMEL
Nov. ’81: Definition of AORS reference formats and codes
Sept. ’82: Reporting criteria, guidelines for data supply and use
FEBR. ’82: Start of transcoding 30,000 event reports
MARCH ’84: Draft agreement AORS
APRIL ’85: Agreement AORS approved by the Commission
JUNE ’85: Discussion on AORS in G.O.A.
OCT. ’85: Discussion on AORS in CGC-5
MARCH ’86: End of transcoding 30,000
APRIL ’86: CGC-5 Ad Hoc Working Group on AORS
### Classification for Reactor Type and Country

<table>
<thead>
<tr>
<th>Type</th>
<th>Number of AORS Reports</th>
<th>Number of Reactor-Years Observed in AORS</th>
<th>Total Oper. Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>PWR</td>
<td>12,034</td>
<td>404 (28%)</td>
<td>1,443</td>
</tr>
<tr>
<td>BWR</td>
<td>11,632</td>
<td>284 (34%)</td>
<td>825</td>
</tr>
<tr>
<td>GCR</td>
<td>885</td>
<td>45 (7%)</td>
<td>646</td>
</tr>
<tr>
<td>HTGR</td>
<td>310</td>
<td>9 (82%)</td>
<td>11</td>
</tr>
<tr>
<td>HNGCR</td>
<td>74</td>
<td>8 (25%)</td>
<td>32</td>
</tr>
<tr>
<td>FBR</td>
<td>36</td>
<td>3 (9%)</td>
<td>33</td>
</tr>
<tr>
<td>Others</td>
<td>-</td>
<td>-</td>
<td>577</td>
</tr>
<tr>
<td><strong>TOTALS</strong></td>
<td><strong>24,971</strong></td>
<td><strong>753 (21%)</strong></td>
<td><strong>3,567</strong></td>
</tr>
</tbody>
</table>

(25% of types followed)

### Country

<table>
<thead>
<tr>
<th>Country</th>
<th>Number of AORS Reports</th>
<th>Number of Reactor-Years Observed in AORS</th>
<th>Total Oper. Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Belgium</td>
<td>128</td>
<td>14 (33%)</td>
<td>43</td>
</tr>
<tr>
<td>France</td>
<td>2,114</td>
<td>124 (59%)</td>
<td>316</td>
</tr>
<tr>
<td>Italy</td>
<td>948</td>
<td>8 (11%)</td>
<td>71</td>
</tr>
<tr>
<td>Netherlands</td>
<td>31</td>
<td>3 (10%)</td>
<td>30</td>
</tr>
<tr>
<td>Sweden</td>
<td>1,907</td>
<td>69 (79%)</td>
<td>87</td>
</tr>
<tr>
<td>USA</td>
<td>19,842</td>
<td>536 (53%)</td>
<td>1,003</td>
</tr>
<tr>
<td>Others</td>
<td>-</td>
<td>-</td>
<td>2,016</td>
</tr>
<tr>
<td><strong>TOTALS</strong></td>
<td><strong>24,971</strong></td>
<td><strong>753 (21%)</strong></td>
<td><strong>3,567</strong></td>
</tr>
</tbody>
</table>

(48.5% of countries followed)

**Component Event Data Bank (CEDB)**

The CEDB is a centralized system, at the European level, for the storage and analysis of failure and repair events of components of NPPs.

**Features:**
- It gives, as output, the component reliability/availability data necessary for reliability analyses.
- Retrieval of the source information for critical reassessment.
- Its classification scheme covers the main classes of components relevant to safety/availability analysis, for various types of NPPs (PWR, BWR, GCR).
- Information coming from the various sources (national banks, NPP operators) is analyzed, homogenized and expressed by a common language coding.
- It will provide a common European data base for reliability analysis (PSA) for NPPs.
CONCLUDING REMARKS

VAST OPERATING EXPERIENCE DATA BANKS WITH EASY ACCESS AND EXHENSIVE CONSULTATION POSSIBILITIES ARE NOW DAYS AVAILABLE: ERDS (AORS AND CEDB)

LEARNING FROM THIS EXPERIENCE IN A SYSTEMATIC AND INTENSIFIED FASHION BY REVIEWING THE RELIABILITY OF SAFETY FUNCTIONS BY MEANS OF INTERACTIVE ANALYSIS TOOLS (CAFTS, SRA),

BETTER (COMPLETENESS, HUMAN ACTIONS, DEPENDENCIES) MODELS FOR "BEST ESTIMATE" SAFETY EVALUATIONS.

IDENTIFICATION OF RELEVANT OPERATING EVENTS TO BE INVESTIGATED IN DEPTH: OPTIMISATION OF FEEDBACK OF EXPERIENCE, ESPECIALLY (OVERLOOKED) PAST EVENTS.

REFERENCES

AORS

Abnormal Occurrences Reporting System Handbook (AORS), JRC-ISPRA Establishment, T.N. 1.05.C1.86.09, February 1986.

CEDB

Component Event Data Bank Handbook (CEDB), JRC-ISPRA Establishment, T.N. 1.05.C1.84.66, October 1984.

CAFTS


SRA

A Short Description of the System Response Analyser Project, JRC-ISPRA Establishment, T.N. 1.05.C1.86.25, March 1986.
Probabilistic Safety Assessment as an Aid to Nuclear Power Plant Management

Brighton, 20-23 May, 1986

"Dependent Failures Data Collection"

P. Humphreys, NCNR, UKAEA

The National Centre of Systems Reliability and the Central Electricity Generating Board have been involved in a joint exercise on the development of improved models of dependent failures.

The project has been structured in three phases. Initially a review of dependent failures models was undertaken with the objective of comparing models for consistency in determining a systems dependent failure probability. The second phase has been directed towards the collection of data from nuclear plant in the UK and USA, while the final phase involves the analysis of the data to improve the basis of refined models of dependent failures.

It is anticipated that the exercise will be of benefit to both NCNR and CEBR in providing causes of dependent failures on which an improved defensive strategy for the prevention and mitigation of such events can be based.

This paper is directed to a discussion of the requirements for the collection of data, the problems associated with collection and some proposals for analysis of data.

Data Collection

Background

The foundation of all the models of dependent failure is the data on multiple failure events that come from actual operating experience. Such data includes not only the record of an event but also information on the design of the system. Present incident/event reporting systems such as the LER's have been the basis for the current techniques even though these data systems do not specifically identify multiple dependent failure events, and detailed system design information must be sought separately.

Data from US operating experiences forms an important part of the input to the exercise. It is essential to obtain data from UK plants for the following reasons:

(1) It would document UK experience and thus provide information on the comparison between UK and US plants.

(2) The documentation of UK experience would provide a basis for future target setting.

(3) Similarities between systems on UK and US plants may permit improvement to the database by contrasting or pooling of information.

Collection requirements

Having decided that a data collection activity on UK plant would be beneficial, work was set in hand to define the purpose and scope of the task:

(1) Formulate definitions of dependent failures, common cause and common mode failures.

(2) Decide which failures and which plant areas/systems/components/procedure should be studied in the task.

(3) Define the quantity and nature of data to be collected for any failure, if available, and what other data should be collected, e.g., plant inventories, information on non-dependent failures which occur in the study period.

Having defined the data collection tasks the selection of candidate stations took place and the detailed activities of the data collection teams were determined.

The problems to be overcome to gain access to data:

1. In order to determine the best sources of data it has been necessary to approach the management of candidate stations in order to explain the purpose of the task, and the potential benefits to be station concerned, for no manager will willingly disturb his operations and maintenance processes without benefit.

2. It has been necessary to explain the organisation of the task, the assistance which would be sought from the station in supervising the collector, and the output from the task, and seek any additional output which the station would welcome.

Definition of data to be collected

The collection of data on a plant wide basis is a major task and for the purposes of the project a sub-system common to all stations was selected for the data collection activity.

In order to clearly define the extent of the system a system boundary was constructed around the components of interest and an inventory of all components within the boundary was collected.

After reviewing the limitations of previous data collection activities, a comprehensive data file was defined describing the data to be collected on each component. This file is shown in Fig. 1.

In the second stage of the data collection activity the historical records of events relating to the components described in the inventory were analysed. The data analysed covered a two year period up to the present time. The analysis of current events is now in progress. To aid the analysis an event data file structure was defined and is shown in Fig. 2.
The problem arising during data collection:

1. Specification of the system boundary - we always have to determine which components lie within the boundary.

2. Data collection is by essentially manual, less important, to give first directions on the type of data to be collected.

3. It was essential to provide a link between the data collector and a site engineer with a good understanding of the plant.

4. The inventory requires considerable data to be collected on each component, and a report card is designed to cover all components, and a supporting document is designed to provide the necessary information.

5. Additional data and material report cards are designed to support the data collector, since much of the information is not immediately available.

In order to provide data for each component, it was decided that a data collection sheet should be constructed.

Data storage and retrieval:

To facilitate storage, retrieval, and analysis of the collected data, it was decided that a data collection sheet should be constructed.

The data collection sheet was designed, one for the inventory data and a second for the event data.

The two sheets were defined, one for the inventory data and a second for the event data.

One recognisable problem with any data collection process is to ensure that all data collected can be directly related to the inventory data. If this is the case, an automatic crosscheck can be used between the two sheets before the sheet is accepted.

The data would have been designed to span the range of analysis and modelling, with a few general fields being used to provide for computer processing.

The two databases have been designed to span the range of analysis and modelling. The database would be used to provide for computer processing.

The results obtained can be used to identify failures leading to the data collector, which is of great importance in identifying failures in the field.

The database is currently being collected and entered into the database.

The database is currently being collected and entered into the database.

The analysis objectives and procedures have been defined.

The analysis objectives and procedures have been defined.

In order to ensure that all actual and potential dependent failures have been detected, a three of four variable computer-based analysis technique will be employed and results compared with those of analysis in 2 above.
The Role of Probabilistic Risk Assessment in Support of Nuclear Plant Operation and Safety: A Northeast Utilities Perspective

Dr. Mario V. Bonaca, System Manager, Reactor Engineering, Northeast Utilities

ABSTRACT

Northeast Utilities (NU) has underway a program to develop, maintain, and utilize for plant support, living Probabilistic Risk Assessments (PRAs) of all of its nuclear power plants. This program is being carried out by an internal staff of fourteen engineers and technicians supported by operations and temporary personnel as needed. The work is being performed on a dedicated interactive computer system. To date, a Level 3 PRA has been completed for Millstone Point 3 (MP3); and Level 1 PRAs have been completed for Connecticut Yankee (CY) and for Millstone Point Unit 1 (MP1). The MP1 and the CT PRAs are being utilized in support of the Integrated Safety Assessment Program (ISAP), which allows the inclusion in the backfit scheduling process of considerations of public safety, economic performance, personnel safety, productivity and external impacts. The PRA models being developed place emphasis on detailed modeling of plant specific hardware, emergency operating procedures, and plant specific equipment reliability data. The models are periodically updated to reflect changes in equipment, procedures, and reliability data; efforts are underway to fully automate this process. Unavailability terms of individual components are being derived from plant specific data bases in order to optimize equipment testing intervals. The models are being utilized to identify plant limitations, and to help optimize improvements. Critical scenarios identified by the PRAs are utilized for plant simulator operator training; operator response to the simulated scenarios provide a valuable benchmark of PRA human factor assumptions. The PRAs are routinely utilized to evaluate proposed plant changes, and in this role they have evolved into powerful systems engineering tools. Critical sequences identified by the PRAs occasionally stimulate a healthy debate among engineers and operators with regard to assumed equipment and personnel performance, thus furthering the understanding of critical operator actions. The purpose of this paper is to explain the reason for such a significant corporate commitment to development and use of PRA, and to expand on present and planned features and applications of the NU PRA program.

INTRODUCTION

Northeast Utilities' (NU) first involvement with PRA dates back to August 1974, when Hurricane Betsy caused significant salt spray to be blown onto the 345 kv insulators in the switchyard of the Millstone Station. This produced arcing that resulted in a complete loss of off-site power. Seaweed and debris began to clog up the cooling water intake structure. For the Millstone Unit 1 (MP1) BWR, which is a 548 MWe with Mark 1 containment, the emergency diesel successfully started and ran, but the emergency gas turbine failed due to human error. This caused the unavailability of the safety grade feedwater system, which is the only high pressure, high capacity makeup system at MP1. The plant was successfully cooled down using the Isolation Condenser, which had a history of maintenance unavailability due to tube leakage.

This event raised several disturbing questions. What if the Isolation Condenser had still been out of service? What if further clogging of the intake structure had eliminated cooling water to the diesel? This event seemed to support the perspective provided by the Reactor Safety Study (WASH-1400), which had showed that the dominant contributors to damaging the reactor core were not the large break LOCA events, for which significant safeguards had been implemented, but events likely to occur during the life of the plant, coupled with plausible failures of decay heat removal systems. This event further implied that a plant compliant with current safety regulations could still have a relatively likely pathway to severe core damage.

These concerns lead to a corporate decision to perform a limited scope decay heat removal system PSA for MP1. This work performed in-house and completed in 1978, identified weaknesses in systems believed acceptable because they met licensing requirements. Improvements were committed for implementation, and a similar study was initiated for Connecticut Yankee (CY), which is a 605 MWe four loop PWR of Westinghouse design, the oldest plant in our system.

The accident at Three Mile Island again highlighted the vulnerability of nuclear power plants to simple failures in decay heat removal systems, coupled with operator error, and reprogrammed PRA on a larger scale. The accident, and the subsequent situation created by the avalanche of individual mandated backfits, raised critical questions within NU with regard to the value of hundreds of generically-inspired plant backfits. Of concern was that, in the process of implementing all these changes, more important changes could be neglected; even worse, that the net result of all these backfits could be a reduction of safety. A growing sentiment developed that there had to be a better way to understand, prioritize, and manage safety issues and to assure that utility originated safety projects would be given equal consideration.
In spite of its known limitations, PSA appeared to be the kind of decision-making tool we needed.

With this background in mind, Northeast Utilities formed a Task Force in the Spring of 1981 to propose various options for developing PSA capability. The following recommendations were provided by the Task Force:

1. Rather than contracting out PSA work to outside consulting firms, a PRA Section would be formed in the Safety Analysis Branch.
2. The PRA Section would be responsible for providing PRA related support to the design and licensing groups.
3. The PRA Section was to develop and maintain living PSA models for all NU operated nuclear power plants.
4. A general five year plan was developed to staff up and initiate PSA models for each of the operating nuclear units, with priority based on the age of the plants (i.e., Connecticut Yankee, followed by Millstone Units 1, 2, and 3).

A goal in developing this capability in-house was to develop full plant models to give us insights on where we stood in terms of meeting proposed safety goals. We would then be in a position to judge the merits of further work in various areas. This strategy obviously differs from that of developing limited scope models, one at a time to respond to narrowly defined issues such as: fire protection, additional isolation valves, improved auxiliary feedwater, etc. Our general concern with that approach was that limited scope PSA models (such as an auxiliary feedwater reliability study) might conclude a particular backfit was not a significant improvement over what existed currently, but it couldn't provide a perspective over whether the existing design was adequate in terms of overall plant safety or whether the proposed design change would be more or less significant than changes in other plant systems in terms of overall plant safety. In summary, the limited scope PSA approach would not provide us with the comprehensive decision making tool we wanted.

The recommendations of the Task Force were endorsed by NU. A Level 3 PSA of MP#3 was performed with Westinghouse (W) in 1982-1983, with close technical coordination from the NU PRA Section. This was because NU was going to be the eventual user of the PSA model, and we felt it was essential to be involved, particularly in areas were judgment calls were being made on data bases and operator actions. This effort included a full scope technology transfer from W to NU, which resulted in the installation of the MP#3 living PSA model on dedicated computers. In 1982, NU issued a corporate safety goal identifying public risk and core melt frequency levels which would be utilized to trigger corrective actions commensurate with the problems identified by PSA models. In 1984, the MP#1 Level 1 PSA was initiated in-house by NU. The model, completed in mid-1985, is currently supporting the MP#1 ISAP. ISAP is a program underway for MP#1 and CY which allows the inclusion in the backfit scheduling process of considerations of public safety (PSA), economic performance (PAM), personnel safety, productivity and external impacts. The CY Level 1 PSA has been performed in-house and was completed by the end of 1985. This model is being utilized to support the CY ISAP. Plans are currently being made for development of a Millstone Point Unit 2 (MP#2) PSA model of similar type.

In 1984, a corporate goal was established for using the living PSA models in all plant support activities (Design Changes, Technical Specifications Changes, Procedural Changes, Training). This required the establishment of procedural links assuring the timely update of the models and their utilization in the plant change process. This procedural upgrade is now nearing completion.

CURRENT STATUS OF NU PSA PROGRAM

Table 1 summarizes the completion status of our PSA models. Plans are currently being made for development of Millstone Unit 2 PSA models of similar scope to CY and MP#1.

The basic scope of the living PSA models being developed by Northeast Utilities is consistent with a Level 1 PSA as defined in NUREG/CR-3379, but provisions have been made so that the models can be added to with passing time. This facilitates the ability in subsequent years to add on analyses of flooding, seismic, etc.). These models when completed and Quality Assured are permanently stored on a dedicated interactive computer system configured by Westinghouse and separate from the main computers used at NU. This computer system includes two interactive graphics display terminals for constructing and quantifying fault tree models and plotting them for documentation purposes.

A unique strength of the NU PSA program is the in-house availability of best-estimate LOCA analysis tools which can be extensively exercised in an iterative process with the PSA analysis in order to study detailed sensitivities to PSA proposed scenarios. The Connecticut Yankee PSA in particular has benefited from this capability. For this plant, we have available a licensed RELAP-5 based plant specific code, RELAP-5, with best estimate capability and Appendix X compliance models. During the performance of the PSA, two LOCA engineers were assigned on a full-time basis to perform
sensitivities of specific scenarios as they were identified by the PSA analysts. The extensive LOCA work has been documented in one of the 5 volumes of the PSA report. This work identified a CT window of non-compliance with applicable regulations in the LOCA area, prompting interim corrective actions to support a temporary NRC exemption from single failure requirements, and is resulting in backfits to be implemented during the next shutdown refueling.

All PSA work is being performed by an internal staff of 14 engineers and technicians, supported by 4 temporary personnel, and by additional plant and engineering personnel as needed. Based on current projections of long term PSA needs, we are planning a 1987 increase in the PSA Section permanent staffing level.

At present, the PSA program has underway a number of activities in addition to the ongoing PSA model development efforts. These activities can be generally categorized as APPLICATION, MAINTENANCE, and DEVELOPMENT activities, and will be described in the following sections.

1. CURRENT PSA APPLICATIONS

As a PSA model of a nuclear unit is completed, the PSA results are evaluated for identification of significant risk outliers and to assess plant safety against the corporate nuclear safety goal, which include criteria of acceptability for core melt frequency and for individual and population risk.

NU's corporate safety goal articulates and quantifies the corporate commitment to protect the health and safety of the public. The Millstone Unit 3 PSA models consider internal and external events, core melt frequency and public risk. The Millstone Unit 1 PSA currently considers internal events and fire. Core melt frequency work on flooding and other external events is currently being added. The Connecticut Yankee PSA currently models internal event core melt frequency (CMF) work on fire risk is currently proceeding. Only limited evaluations are performed of containment performance, including containment bypass (V) sequences. Although individual and public risk are not explicitly derived, methodology exists to estimate these impacts based on parameters affecting core melt (e.g., initiator type, timing, safeguards availability). Thus, the focus of our current PSA work is on core melt frequency quantification, its extrapolation to risk, and its reduction through identification and elimination of risk areas. At present, this appears to be the best possible use of PSA, as an engineering tool for evaluating front line system performance, operator action, and potential problem areas. It is, in fact, in this function that our plant specific PSA models are proving most effective.

1.1 RESOLUTION OF PSA IDENTIFIED PLANT VULNERABILITIES

As risk contributors are identified, they are divided into two main categories: those which must be resolved on a priority basis due to their significance and are not considered in our backfit program. All identified issues are tracked towards resolution using existing tracking systems.

1.1.1 DISPOSITIONING OF SIGNIFICANT VULNERABILITIES

Each plant specific PSA of our older nuclear units (Connecticut Yankee, Millstone Unit 1) has identified plant unique vulnerabilities which added up to high CMF when compared to our corporate safety goal (10^-7/yr, median value). The identified shortcomings pointed to inadequacies of early designs, and were readily recognized as unacceptable to our engineers, operators, and managers irrespective of the ultimate core melt frequency results.

Contrary to these observations relative to CY and MP-1, the Millstone Unit 3 PSA did not identify plant specific weaknesses which could be identified as significant risk outliers. The main reason for this difference appears to be tied to the vintage of these plants. Millstone Unit 3 is a new plant, which was designed to comply with extensive redundancy and separation requirements, and was extensively supported at the design stage by PRAAs and system interaction analyses.

Examples of significant vulnerabilities identified for CY and Millstone Unit 1, and their relative contribution to core melt frequency, are summarized in Tables 2 and 3. The most significant finding at CY involved complex dependencies of critical equipment on a single motor control center, MCCS. Loss of MCCS would result in over 20 cascading consequences, one of which involved the auto start of the charging pumps with concurrent closure of the RCS isolation valves. This would cause the Volume Control Tank (VCT) to empty in approximately 1/2 core melt time, which would result in a major failure. The short term fix involved the implementation of an automatic pump...
trip on loss of MCCs. This was further enhanced by development of an emergency procedure for loss of MCCs and by significant operator training on the plant specific simulator prior to plant restart from refueling. Long term resolution involves the implementation of a new MCC to accept one half of the loads carried by MCCs.

A significant finding of the CY PSS was the identification of a narrow window of small break LOCAs for which the ECCS systems would be ineffective during the high pressure recirculation phase. Based on the PSS, alternate equipment was identified which could successfully perform during recirculation, emergency procedures were modified and operators re-trained prior to plant restart following shutdown refueling. Throughout the process, the PSS was continually used to define potential problems, focus attention on best possible solutions, and verify correct implementation.

A critical dependency of both CY diesels cooling systems on a single component was also discovered; failure of this component upon loss of off-site power would have resulted in a loss of cooling to both diesels and consequent station blackout. The immediate corrective action involved locking open the valves controlling service water cooling to the diesels after verifying that this would not result in unacceptable diesel cooling, and the subsequent rewiring of the electrical controls.

The most significant finding for MPFI is that a full 2/3 of core melt frequency is due to limitations in long term cooling systems. Although consistent with their licensed design basis, the shutdown cooling systems of MPFI appear vulnerable to failures which comprehensively reduce the overall reliability of these systems to levels below that acceptable to NRC.

The significance of these shortcomings to NU was such that immediate corrective actions were taken to resolve them. In some cases, this required only procedural changes, in other cases hardware repairs were required, that at CY were implemented during the past shutdown refueling and prior to returning to power operation. In the case of the CY CC-5 modifications, the changes were designed, equipment procured and installed, and the system tested along with the completion of all required safety evaluations in a 1 month time frame under "emergency" work orders.

In view of the dozens of other projects ongoing at the time, and the one to two years lead times generally associated with such changes, this was an outstanding accomplishment reflecting the importance placed by NU on the PSA findings.

Where the required backfit may involve hardware requiring long procurement lead times, such as for the resolution of the MPFI long term cooling limitations, immediate corrective action may actually mean implementation during next shutdown refueling. In this case, by "immediate" is meant that the change takes priority over all other planned changes. If this creates a conflict with NRC mandated backfits, the proposed change is entered into the Integrated Safety Assessment Program (ISAP), which is specifically designed to establish a priority ranking of proposed backfits, visible to the NRC, supported by PRAs, and therefore providing a basis for negotiations with the NRC. As an example, the NRC has fully concurred with our proposed resolution of the MPFI long term cooling issue on a priority basis.

1.1.2 RANKING OF OTHER PROPOSED BACKFITS

All other items identified as significant by the MPFI and CY PRAs, as well as all other proposed design changes for these plants, are evaluated to provide the safety input to the Integrated Safety Assessment Program (ISAP), which is presently underway with the NRC for CY and MPFI. This program allows the inclusion in the backfit scheduling process of considerations of public safety (PRA), economic performance (RAM), personnel safety, productivity, and external impact. Desired objectives of the ISAP ranking process, which is the end result of the program, are prioritization of safety issues, formal NRC acceptance of NU identified plant specific safety issues, and resource allocation. ISAP rankings for all current MPFI projects have been completed. The public safety input to the ranking process was obtained by determining the net Ram-Ram reduction associated with each proposed backfit during the remaining plant operating life. Table 4 summarises the value of NRC and NU initiated backfits from a public risk reduction standpoint. The table clearly shows that, in general, the NU initiated backfits based on plant specific insights contribute more to risk reduction than the NRC initiated generic
backfits. Even more impressive is the wide spread in
Man-Ram reductions between most of the NRC initiated
backfits and the backfits identified as important by
the ISAP process. This wide spread reduces concerns
with regard to subjectivity in the PRA ranking process
and uncertainties in the PRA results.

The plant specific PRAs developed for CY and MPP1 were
critical to the success of the ISAP program. In this
role, they have proven to be invaluable. Their
availability has allowed NU to prioritize over 50
individual backfits for MPP1 and 20, to date, for CY.

The success of this undertaking in improving our
understanding of safety issues and in dealing with the
NRC is such that plans are underway for the
development of similar programs for Millstone Unit 3
and Millstone Unit 2.

1.2 INTEGRATED SAFETY EVALUATIONS

U.S. regulations (10-CFR-50.59) require that, at the end of
the design process and prior to the implementation of a plant
change, a Safety Evaluation be performed to determine if the
proposed change involves an unreviewed safety question. The
intent of this regulation is to obtain NRC review and
concurrency of changes which, although safe, may expand the
licensed bounds of the accident analysis.

NU uses this evaluation first as a means of determining that
the change does not represent an unacceptable degradation of
safety, and second, if determined to be safe, to assess if it
is an unreviewed safety question. PSA is being utilized in
this type of application. Table 5 provides a summary of the
key PSA supported safety evaluations performed over the past
couple of months.

This role of PSA is emphasized by the NU procedural framework
requiring that the Safety Analysis Branch, which includes the
PRA Section, performs an integrated safety evaluation of all
proposed changes. These limited PSA evaluations occasionally
indicate that a proposed change degrades safety and should
not be implemented as is. Unfortunately, this assessment is
provided at the back end of the design change process, often
too late for further design changes to be incorporated within
the existing schedule. This causes committed backfits, some
of which were being carried out to comply with NRC
requirements, to have to be postponed, occasionally creating
regulatory problems.

An example of this type of situation is the recent
engineering effort to upgrade the undervoltage protection
logic for the AC power system at MPPI. This logic is
designed to sense loss of off-site power for both power
tran, load shed all class 1E buses, start the emergency
power sources, and reload emergency equipment. The change
to the existing system was designed to increase separation of
the two power divisions. This objective was achieved, but
the configuration of the new design significantly increased
the probability of station blackout. Therefore, the proposed
change could not be implemented. The PSA was then used in an
iterative mode to optimize the proposed hardware solutions.
Modified logic will be implemented during the next shutdown
refueling.

This is just one of the many examples of unique insights
provided by PSA into proposed design changes. Because of
this proven effectiveness, and to prevent identification of
design deficiencies at the end of design process, the demand
for PSA evaluations by engineering disciplines within NU has
increased well beyond the present support capability of the
Section.

1.3 PSA IN SUPPORT OF DESIGN CHANGES

The fact is, PSA is proving to be the most effective system
engineering tool presently available to NU. This should not
come as a surprise, as PSA incorporates and integrates some
of the most effective system engineering tools available
today, such as PRA. A systems engineering perspective is
in fact badly needed in support of the many plant design
changes being implemented, in order to optimize design
solutions at the system level while providing assurance that
a potential performance degradation is not being accidentally
introduced as a side effect. PSA provides this perspective,
and as a systems engineering tool represents an improvement
over those utilized by the original plant designers. This is
because PSA includes considerations of operator actions, of
actual component reliability data and of plant operating
practices. Some of theoriginal design analyses tended to
concentrate on individual system performance, with little
attention given to operator actions. Yet, in U.S. operating
philosophy, the operator is the ultimate safeguard, and an
adequately designed and implemented ECCS system will not do
very well if a misinformed or inadequately trained operator
will take it out of service when it is needed.
Many examples already exist of the effectiveness of our PRAs in evaluating and occasionally improving proposed design changes. Examples are provided in Table 6.

A planned MP1 AC power backfeed from MP2 for Appendix B protection in case of switchgear fire was found to yield marginal benefit in terms of public risk reduction. An opportunity was identified by the PRA team for a minor project change which would allow us to also address station blackout resulting from a loss of off-site power. With this change in scope, the change is shown in Table 4 as providing significant benefit in terms of risk reduction. Similar considerations can be made for the Appendix B initiated changes to the critical motor control center at CY previously discussed in this paper. PSA improvements to the project provided further reduction in public risk.

PSA was similarly successful in optimizing, with NPC concurrence, required modifications to the scram discharge volume tank water level instrumentation of MP1, following the June 1980 Brown's Ferry event, when a partially filled scram discharge volume went undetected and prevented full control rod insertion. The NPC hypothesized level sensor failure and thus proposed that all BWRs install diverse level sensors. The PSA analysis showed that at MP1, the risk that the discharge tank would fill without an anticipatory reactor trip was dominated by the many manual root valves being frequently manipulated in a high radiation area by personnel for calibration and maintenance purposes. Level instrumentation at MP1 is of a slightly different and very reliable type, as shown by no experienced failures in 15 years of operation. NPC recognized the safety benefit resulting from NU's proposed alternate design change and readily approved it.

Because of this effectiveness of PSA, and as our model development phase comes towards completion, more of our personnel are being assigned to support the front-end of the design change process, to help optimize design changes, rather than to show the inadequacy of the changes at the end of the process.

1.4 TRAINING AND EMERGENCY PROCEDURES

Information concerning critical operator actions identified by the plant specific PRAs has been incorporated into training plans and drills on the plant specific simulators at the NU Training Center. A significant number of emergency procedures have been modified, and new ones have been generated to reflect critical findings of the plant specific PRAs.

An especially intense effort in the procedural area followed the recent completion of the CY PSB. The PSB identified a narrow window of small break LOCA's for which the ECCS systems would be ineffective during the recirculation phase. Alternate equipment was identified which could successfully perform during recirculation, and emergency procedures had to be modified. The operators were trained prior to plant restart following shutdown refueling.

A poignant example of the effectiveness of the combination of PSA insights and plant specific simulator training is provided by the activities which followed the PSA identification of the consequences of loss of Motor Control Center 5 at CY. While most consequences of loss of MCC-5 appeared recoverable, the PSA engineers were concerned about the ability of the operators to identify this initiating event and to take one critical action, to trip the high pressure charging pumps, (which come on automatically upon loss of MCC-5) prior to emotting the VCT in about 1 minute. Plant personnel argued that indeed the operators would take timely actions, and pressed for postponing plant modifications to address this problem to the 1987 shutdown refueling. The following day, the loss of MCC-5 event was simulated on the CY specific simulator during training of a full shift of operators. The simulator confirmed the PSA predictions, and showed that the operators had difficulty in timely identifying the event, and thus did not timely trip the charging pumps. Consequently, trip of the charging pump upon loss of MCC-5 has been implemented prior to return to power from refueling; a loss of MCC-5 emergency procedure has been developed and implemented, and simulator training has been provided to all shift operators.

1.5 USE OF PSA IN IMPROVING SURVEILLANCE PROCEDURES

The NU plant specific PSAs have identified a number of areas where surveillance procedures can be improved. Table 7 summarizes a number of cases where plant reliability and safeguards availability have been improved during the past year via changes in test intervals.

As an example, the MP1 PRA identified the MSIV closure event as a dominant contributor to certain core melt sequences. Plant specific records indicated that 40% of the frequency of
MSIV closure was due to events occurring during the 10A MSIV closure RPS trip function test required by Technical Specifications and performed monthly during full power operation. The PSA model was utilized to evaluate if the reduction in core melt frequency due to reducing challenges from MSIV closure events would outweigh any potential increase in core melt frequency due to less frequent testing of a portion of the reactor protection system. The evaluation indicated that the monthly test should be replaced by simple changes to the quarterly MSIV closure tests (performed at reduced power levels), to simultaneously test the operability of the MSIVs and the reactor trip on greater than 10A MSIV closure. A net reduction in core melt frequency was projected if surveillance was reduced.

In some cases, the PRA based review of the surveillance procedure showed that the tests as performed did not achieve the objective of the test. Simple modifications were, therefore, proposed and implemented. As an example, it was found that testing of the CY main steam trip valves (MSIV) was not systematic. The procedure specified to trim any of the 2 of 4 high steam flow indication channels. Testing of all 4 channels was not assured, as confirmed by the review of past test records. Changes to the procedures are underway.

In other cases, these reviews lead to more frequent testing. This is occurring for the ECCS systems of MP6, where the PSS is being utilized to optimize surveillance intervals. The current MP6 In-Service Test (IST) program, based on ASME Section 11 requirements, did not appear to provide optimal intervals based on actual mean time to failure. A significant effort was undertaken to perform approximately 20 separate calculations, using PRA models which had to be updated to reflect final design and proposed IST program. The results of this study confirmed that the ASME requirements do not appear in all cases to be optimized to reflect mean times between failures. An effort is underway to optimize the ECCS surveillance intervals with the PRA for inclusion in the IST program.

2. PSA MAINTENANCE ACTIVITIES

The maintenance of the PSA models is essential to ensure they continue to provide an accurate description of the plant. Plant changes (hardware and procedures) and operational data (maintenance, run time, and equipment failure rates) are being collected to update the PSA models. The MU procedural framework is used to collect plant design change documentation.

The use of plant specific reliability data is critical in assuring the fidelity of the PSA models. The plant-specific data alone provides significant insights into many plant systems. By using this data, not only is attention given to problems inherent to the plant, but also credit is taken for above average equipment performance attributable to activities such as a strong preventive maintenance program. This assures that applications of the PSA model to the design process and for operations input are made with knowledge of existing plant reliability and that such activities are directed to areas needing the most attention.

Significant resources were expended to obtain the plant-specific reliability information, using diverse sources of data such as plant operating and maintenance logs for both MP6 and CY. This process had generated raw numbers of actual component or system failure, numbers of demands or in-service hours, and total run hours for each individual pump since initial plant operation. This information, and the derivation of related uncertainty distributions has previously been published in Reference 1. Maintenance unavailabilities of systems and components were systematically analyzed to provide means and variances for many key plant systems and components. Tables 8 and 9 provide examples of raw data available for MP6.

It is noticeable that such effort had provided a number of insights into system reliability without even having performed fault tree analysis. For MP6, for example, this plant specific data base indicates that MOV failure to open (5 failures in 369 demands) is much higher for MOVs inside drywell than for those outside the drywell, that MOV failure to open is significantly higher than ECCS pump failure to start and that electrical breaker failure to close is insignificant (9 failures in 45,571 demands). This information is very different from the engineering judgment based data provided by WASH-1400, which attributes the same failure rate to all of the above components. These insights are becoming so valuable, that periodic updates of this data base are planned to reveal any trends in the reliability data.

3. DEVELOPMENTAL ACTIVITIES

A number of developmental activities are underway internally and through contractors to further improve available software and data base information.

In order to utilize the PSA models to optimize design changes, very fast turnaround is required to support the schedule. An effort is underway to upgrade the MP6 and the CY reliability data base software to automate the PSA models. The software under
development will automatically change the component unavailability calculations in the PSA to reflect changes in reliability data, in hardware or in testing procedures. The program will automatically requantify affected fault trees and event trees to yield new risk numbers.

Recognising that human error probabilities constitute the area of greatest uncertainty in the whole PSA technology, we are working with EPRI to develop techniques for better treating human reliability. We are presently entering a joint program to utilize plant specific simulator data to develop, refine, and benchmark operator response models.

Efforts are underway to better define and support the failure rate uncertainty distribution for several plant systems and components.

The extensive plant specific data bases for MP81 and CY provide substantial unavailability information on identical components (in similar environments) which have been subjected to different testing intervals. This information is being correlated in an attempt to separate time dependent vs. demand unavailabilities, in order to optimize testing intervals, dependent on the dominance of either term on the overall component unavailability.

A significant effort is underway to further validate component unavailabilities being used in the PSAs. For many components, insufficient failure experience and statistics exist to allow generation of uncertainty distributions based on classical statistics. NU has, therefore, developed Bayesian updates of WASH-1400 type data using existing plant specific data (Reference 1). An effort is underway to compare unavailabilities of components as predicted with the Bayesian update approach with the predictions of classical statistics. Figure 1 provides an example of the kind of results being obtained for individual components. By incorporating into different unavailability models actual component failure rates over 160 months of operation, the unavailability predictions tend to converge, improving confidence in the values being used in the PSA models.

CONCLUSIONS

The NU PSA program has clearly shown that PSA works, both as an internal decision making tool, and as a safety analysis tool for dealing with the regulators. From its beginning and through the model development phase, our PSA program has identified significant opportunities for reducing risk at our power plants. The PSAs have helped us become conversant with safety issues affecting our plants, providing us with a perspective on risk, and with the ability to make intelligent decisions regarding safety, rather than blindly following regulatory requirements. Our commitment to understanding safety issues, discussing them with the regulators, and taking action commensurate with the significance of the findings follows from our conviction that safety is our business as much as it is the regulators business. The vulnerabilities identified by our PSAs show that we cannot become complacent, but must continue to apply our resources to further identify safety concerns and bring them to proper resolution. We simply cannot afford nuclear accidents. In this pursuit of safety, nothing is to be gained by the adversarial approach which has often characterized the utility - regulatory interface in the United States, since safety is our common business. Our PSAs have proven to be engineering tools capable of opening a constructive dialogue with the NRC, and we at NU are committed to continue pursuing their use in this role.

Table I
Status of PSA Models for
Northeast Utilities Nuclear Power Plants

<table>
<thead>
<tr>
<th>Plant</th>
<th>Commercial Operation</th>
<th>PSA Model Completion</th>
<th>PSA Model Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>1825 MW, 4-loop</td>
<td>Westinghouse PWR</td>
<td></td>
<td>Fires</td>
</tr>
<tr>
<td></td>
<td>large dry containment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Millstone Unit 1</td>
<td>Dec. 1970</td>
<td>July 1985</td>
<td>Internal Events</td>
</tr>
<tr>
<td>2011 MW, BWR 3</td>
<td>General Electric</td>
<td></td>
<td>Fires</td>
</tr>
<tr>
<td></td>
<td>Inerted Mark I containment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Millstone Unit 2</td>
<td>Dec. 1973</td>
<td>1988 *</td>
<td>Internal Events</td>
</tr>
<tr>
<td>2700 MW, 2-loop</td>
<td>Combustion Engineering PWR</td>
<td></td>
<td>Fires</td>
</tr>
<tr>
<td></td>
<td>large dry containment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Millstone Unit 3</td>
<td>May 1985</td>
<td>Aug. 1983</td>
<td>Internal Events</td>
</tr>
<tr>
<td>3011 MW, 8-loop</td>
<td>Westinghouse PWR</td>
<td></td>
<td>External Events</td>
</tr>
<tr>
<td></td>
<td>subatmospheric containment</td>
<td></td>
<td>Containment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Consequences</td>
</tr>
</tbody>
</table>

Table 2
Contribution of Unique Plant Features to Core Melt Frequency at Connecticut Yankee

<table>
<thead>
<tr>
<th>BEFORE CORRECTIVE ACTIONS</th>
<th>AFTER CORRECTIVE ACTION ALREADY TAKEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of Motor Control Center</td>
<td>60%</td>
</tr>
<tr>
<td>Single Injection Path for High Pressure ECC Recirculation</td>
<td>7%</td>
</tr>
<tr>
<td>Loss of DC Power</td>
<td>3%</td>
</tr>
<tr>
<td>Others</td>
<td>26</td>
</tr>
</tbody>
</table>

(1) Absolute Contribution to Core Melt Frequency Was Not Changed.
| TABLE 5 | TABLE 6 |

**INTEGRATED SAFETY EVALUATIONS**
| RECENTLY PERFORMED BY PRA SECTION |

**MILLSTONE UNIT 1**
- Undervoltage Logic Changes
- Gas Turbine Start Logic Modifications
- Diesel Shutdown Logic Modifications
- MOV Replacement
- EED Compliance of MOVs

**CONNECTICUT YANKEE**
- Loss of MCC-5 Protection
- Procedures for Alternate Means of High Pressure Recirculation

**MILLSTONE UNIT 3**
- Diesel Shutdown Logic Modifications

**PRA BASED DESIGN EVALUATIONS**

- Millstone Unit 3 Hydrogen Igniter
- Millstone Unit 1 Scram Discharge Level Instrumentation
- Millstone Unit 3 Reactor Cavity Flooding
- Millstone Unit 3 Chemical Volume Control System (Boron Dilution)
- Millstone Units 1, 2 and Connecticut Yankee Fire Protection
- Millstone Unit 1 Decoy Heat Removal Systems
- Connecticut Yankee Decoy Heat Removal Systems
- Connecticut Yankee Off-Site Power Transmission Tower Placement
- Connecticut Yankee Refuel Water Storage Tank Air Vent
- Millstone Unit 3 Service Water System (Flooding Protection)
- Millstone Unit 1 Loss of Normal Power Logic Modifications
- Millstone Units 1 and 2 Reactor Protection System Logic
- Millstone Unit 1 AC Power Backfeed from Millstone Unit 2
- Millstone Units 1, 2, and 3 Shared On-site AC Electrical Supplies
- Connecticut Yankee Appendix R Modification Improvements
- Millstone Unit 3 Diesel Lube Oil Coolers Evaluation
TABLE 7

RECENT IMPROVEMENTS IN PLANT RELIABILITY AND SAFEGUARDS
AVAILABILITY VIA PRA SUPPORTED TESTING CHANGES

MILLSTONE UNIT 1
- LPCI Pump Lube Oil Cooling
  Function Verified by Tests
- Optimization of Emergency
  Service Water Pump Test
  Frequency
- Optimization of MSIV
  Surveillance Intervals (10% Closure Test)

CONNECTICUT YANKEE
- Optimization of APW Valve
  Testing Intervals and Preventive Maintenance Procedure
- Systematic Testing of MSTV's
- Testing of Charging Pump Lube
  Oil Cooler Fans

MILLSTONE UNIT 3
- Evaluation of ECCS Surveillance Intervals
- Evaluation of Interruptable
  Power Supply for MSIV Control

---

TABLE 8

RAW COMPONENT FAILURE DATA COLLECTED AT MILLSTONE UNIT I

<table>
<thead>
<tr>
<th>Component/Failure Mode</th>
<th>Failures</th>
<th>Demands</th>
<th>Mean Q</th>
<th>Upper Bound Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOVs (outside drywell)</td>
<td>Fail to open 29 5497 5.28E-3 6.62E-3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fail to close 19 5497 3.46E-3 4.80E-3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MOVs (inside drywell)</td>
<td>Fail to open 5 369 1.36E-2 2.57E-2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fail to close 7 369 1.90E-2 3.39E-2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECCS check valves</td>
<td>Fail to open 0 1272 7.86E-4 1.51E-3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fail to close 0 1272 7.86E-4 1.51E-3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feedwater check valves</td>
<td>Fail to open 0 676 1.48E-3 2.84E-3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fail to close 3 676 4.44E-3 1.04E-2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECCS pumps</td>
<td>Fail to start 0 954 4.05E-3 2.01E-3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Water pumps</td>
<td>Fail to start 0 827 1.21E-3 2.32E-3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency Service Water pumps</td>
<td>Fail to start 9 258 3.49E-2 5.84E-2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R.B.C.C.W. pumps</td>
<td>Fail to start 0 901 2.00E-3 3.83E-3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shutdown Cooling pumps</td>
<td>Fail to start 3 299 1.16E-2 2.72E-2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T.B.S.C.C.W. pumps</td>
<td>Fail to start 0 414 2.42E-3 4.64E-3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feedwater pumps</td>
<td>Fail to start 0 851 2.22E-3 4.25E-3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Condensate Booster pumps</td>
<td>Fail to start 1 252 3.97E-3 1.95E-2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Condensate pumps</td>
<td>Fail to start 0 239 9.18E-3 8.04E-3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency Condensate Transfer pumps</td>
<td>Fail to start 0 150 5.33E-3 1.22E-2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**TABLE 8 (CONT'D)**

**RAW COMPONENT FAILURE DATA COLLECTED AT MILLSTONE UNIT I**

<table>
<thead>
<tr>
<th>Component/Failure Mode</th>
<th>Failures</th>
<th>Demands</th>
<th>Mean Q</th>
<th>Upper Bound Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>C.R.D. pumps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fail to start</td>
<td>1</td>
<td>342</td>
<td>2.92E-3</td>
<td>1.14E-2</td>
</tr>
<tr>
<td>Diesel Driven Fire pumps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fail to start</td>
<td>8</td>
<td>158</td>
<td>5.06E-2</td>
<td>8.73E-2</td>
</tr>
<tr>
<td>Motor Driven Fire pumps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fail to start</td>
<td>0</td>
<td>158</td>
<td>&lt;5.33E-3</td>
<td>1.22E-2</td>
</tr>
<tr>
<td>8.10KV breakers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fail to operate</td>
<td>3</td>
<td>38,333</td>
<td>8.77E-5</td>
<td>2.05E-4</td>
</tr>
<tr>
<td>BBBV breakers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fail to operate</td>
<td>6</td>
<td>11,238</td>
<td>9.38E-4</td>
<td>9.95E-4</td>
</tr>
<tr>
<td>Diesel Generator</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fail to start</td>
<td>3</td>
<td>652</td>
<td>4.60E-1</td>
<td>1.08E-2</td>
</tr>
<tr>
<td>Gas Turbine Generator</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fail to start</td>
<td>28</td>
<td>834</td>
<td>3.36E-2</td>
<td>3.64E-2</td>
</tr>
<tr>
<td>Main Feedwater System</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>operate post-scram</td>
<td>1</td>
<td>97</td>
<td>1.03E-2</td>
<td>4.03E-2</td>
</tr>
</tbody>
</table>

*Note: For cases of no failures, one failure is assumed for computations.*

**TABLE 9**

**RAW COMPONENT HOURLY FAILURE RATE DATA COLLECTED AT MILLSTONE UNIT I**

<table>
<thead>
<tr>
<th>Component/Failure Mode</th>
<th>Failures</th>
<th>Hours</th>
<th>Mean λ</th>
<th>Upper Bound λ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feedwater Reg. valves</td>
<td></td>
<td>158,979</td>
<td>1.21E-4</td>
<td>1.70E-4</td>
</tr>
<tr>
<td>fails to operate</td>
<td>18</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Water pumps</td>
<td></td>
<td>238,372</td>
<td>3.77E-5</td>
<td>6.32E-5</td>
</tr>
<tr>
<td>fails to run</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R.B.C.C.W. pumps</td>
<td></td>
<td>117,883</td>
<td>8.48E-5</td>
<td>3.31E-5</td>
</tr>
<tr>
<td>fails to run</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shutdown Cooling pumps</td>
<td></td>
<td>15,050</td>
<td>6.64E-5</td>
<td>1.28E-4</td>
</tr>
<tr>
<td>fails to run</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T.B.S.C.C.W. pumps</td>
<td></td>
<td>111,704</td>
<td>8.95E-5</td>
<td>3.50E-5</td>
</tr>
<tr>
<td>fails to run</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feedwater pumps</td>
<td></td>
<td>110,029</td>
<td>9.09E-5</td>
<td>1.75E-5</td>
</tr>
<tr>
<td>fails to run</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Condensate Booster pumps</td>
<td></td>
<td>179,390</td>
<td>5.02E-5</td>
<td>8.40E-5</td>
</tr>
<tr>
<td>fails to run</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Condensate pumps</td>
<td></td>
<td>188,787</td>
<td>5.30E-5</td>
<td>1.02E-5</td>
</tr>
<tr>
<td>fails to run</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C.R.D. pumps</td>
<td></td>
<td>101,652</td>
<td>9.84E-5</td>
<td>1.89E-5</td>
</tr>
<tr>
<td>fails to run</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diesel Generator</td>
<td></td>
<td>1,018</td>
<td>9.82E-4</td>
<td>3.84E-3</td>
</tr>
<tr>
<td>fails to run</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gas Turbine Generator</td>
<td></td>
<td>5,697</td>
<td>1.76E-4</td>
<td>6.86E-4</td>
</tr>
<tr>
<td>fails to run</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Battery Charger</td>
<td></td>
<td>229,488</td>
<td>2.18E-5</td>
<td>4.29E-5</td>
</tr>
<tr>
<td>fails to run</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Note: For cases of no failure, one failure is assumed in computations.*
1. PLANT INFORMATION AND THE OBJECTIVES OF THE STUDY

Beznau nuclear power plant is a twin unit station. The reactor coolant system is a two loop pressurized water reactor (PWR) designed by Westinghouse Electric Corp. Each unit has an output of 350 MW electric and has two identical turbines supplied by Brown Boveri Corp., Baden. The average availability of each plant is well over 80 percent. Unit I reached full power in 1969 and unit II in 1971. The design of both units is based on the 1965 PWR technology.

The nuclear power plant Beznau is owned and operated by the Nordostschweizerische Kraftwerke AG (NOK), Baden, Switzerland.

According to the Swiss law the plant owner has the liability to upgrade the plant to the state-of-the-art all the time as far as necessary and reasonable. In 1978 the Swiss Regulatory Authority (HSK) asked NOK to think about such adjustments, particularly with respect to external events.

After the first evaluation both parties NOK and HSK came to the conclusion, that the most effective way for fulfilling these legal requirements is a solution in the form of add-on bunkered safety systems. The government then asked for a more specific project based on the add-on bunker concept.

In order to meet these requirements, NOK initiated a backfit project called NANO (Nachrüsten Notstandszeit/Notstromversorung). The main features of the NANO project are:
- Improvement of plant protection against external events such as earthquakes, lightening, airplane crash, etc.
- Improvement of plant safety against fire
- Upgrading of the Emergency Core Cooling System
- Redundant Emergency Feedwater System
- Upgrading of the Emergency Electric Power Supply
- Installation of an external recirculation loop.

NOK worked out a concept and placed orders with
- Kraftwerk-Union
  and
- Westinghouse/BBC consortium.

In 1983 the Kraftwerk-Union (KMU) and the Westinghouse/BBC consortium developed two separate projects based on the NANO-Konzept 1982. All the three projects had the same unacceptable features.
- Very high costs - higher than the original price of the entire plant
- Very long schedule - a projected erection time of nine years
- NOK was not convinced of the cost - effectiveness of this backfit effort.

In view of this NOK Management decided to reevaluate the entire project with special consideration to the following aspects:
- How far the regulatory regulations which are generic and are intended for new plants address to Beznau specific requirements?
  It is known that there exists a very complex relationship between the plant hardware, software and the operating staff. It is questionable whether regulatory guides published by different departments can envelope this man-machine interaction.
- Which are the cost - effective alternatives available to NOK and how do they effect the plant safety?
- Are all the dominant contributors to the plant risk identified?
- What about the contributors to the utility's investment risk?

In order to answer these questions, NOK decided to perform a plant and site specific Probabilistic Risk Assessment Study. After a careful evaluation of all the five bids; Pickard, Lowe and Garrick were commissioned with the analysis of the plant systems and Westinghouse was contracted to perform core and containment analysis.

The main objectives of this PRA study are:
- to analyse in a comprehensive manner the major weak points in the existing plant design for internal as well as external initiating events,
- to identify, analyse and quantify the potential for sustaining core damage,
- to assess the increase in plant safety resp. reduction in risk associated with the envisaged NANO backfit project,
- gain insights for the optimisation of technical specifications,
- permit follow on analysis of financial risk,
- to study the core and containment behavior under accident conditions.

2. TECHNICAL APPROACH

The Beznau Risk Analysis is divided in three phases. The Phase A consists of two plant configurations:

1. a model of the plant as it exists and is operated at the start of the study on Oct. 1983 and
2. a model of the existing plant modified by KWU-NANO backfit concept.

The purpose for performing Phase A is:
- to identify key areas of the plant model where refinements should be emphasized in Phase B and
- to provide an opportunity to the plant staff to review the identified weak points and to determine any action to be taken depending on the cause of each weak point.

After NOK's review of the Phase A results (refer to section 3) and reaching a mutual agreement on the weak points identified, NOK decided to reanalyse Phase A hereafter referred to as Phase AI with the following modifications and extensions:

- incorporate into Phase A plant "As-Is" model the modifications agreed upon between PLG and NOK (Refer to Table 1),
- analyze the revised plant "As-Is" configuration modified with "KWU-NANO" backfit design,
- analyze the revised plant "As-Is" configuration modified by "NANO-ReRe" concept.

The basic difference between the "NANO-ReRe" and "KWU-NANO" backfit concept is that "NANO-ReRe" is a single train and "KWU-NANO" is a two train concept.

The complete Phase AI model for the three configurations is shown in Fig. 1 in terms of its event tree segments and pinch points.

The results of the Phase AI analyses are given in section 3.
This Phase A analysis served as a screening analysis to help define the backfit configuration for the Phase B analysis. The detailed analyses in Phase B were then performed for the Plant "As-Is" configuration and for the "NANO-ReRe" configuration defined as Konzept 85.

For a risk assessment study to be really plant specific and useful for the plant risk management it is very important that the details with respect to the specific plant are considered. In the following we will show how it was done in the case of BERA.

A. DATA COLLECTION

Nuclear power plant Bezau has approximately over 26 years of operating history and that means an enormous amount of data. Table 2 summarizes the information reviewed. After a thorough review of the plant operating history a detailed, Bezau-specific data base was developed for initiating events, frequencies, component failure rates, component maintenance un-availabilities and component common cause failure parameters. A Bayesian update was performed where Bezau - specific data could be evaluated. For this update a PUG proprietary data base was used to develop the prior evidence.

B. MODEL OVERVIEW AND PLANT DAMAGE STATES

The BERA plant model consists of four linked event tree stages as shown in Fig. 1. The support system model includes the plant electric power event tree and the plant auxiliary systems event trees. The frontline systems model (Phase A1) includes the event trees for transients and loss of coolant accident sequences and the event trees for the long-term recirculation cooling phase. The plant modification for the "NANO-KMU" concept or for the "NANO-ReRe" concept is manifested in two ways. For the plant auxiliary systems, a separate event tree was developed for each concept that includes all the backfit modifications with respect to the support systems. The NANO-Notstrom-Diesel is included in the electric power event tree. The frontline systems event trees address core cooling functions, which remain unchanged for the "NANO-KMU" and "NANO-ReRe" concept, except that the top event success criteria change to reflect the added components for the feedwater, charging, and ECCS functions of NANO.

In the following each segment of the model is discussed.

Support System

A support system does not directly perform a vital core or containment protection function after reactor trip but is necessary to support the operation of the systems that perform the frontline functions.

Four separate support system event trees had to be developed to accurately represent the configuration of the various support systems. These event trees are:

- Electric power systems event tree
- The plant "As-Is" auxiliary systems event tree
- Auxiliary systems event tree for the plant with "NANO-KMU"
- Auxiliary systems event tree for the plant "NANO-ReRe"

For each plant configuration and for each initiating event, the plant support systems model was quantified.

Frontline Systems Model

For the Phases A and A1, event sequence models were developed for transient event sequences, for small LOCA and large LOCA event sequences. Specific event sequence models for steam generator tube rupture, ATRS and steam line break were reserved for more detailed Phase B, because these sequences have not significantly contributed to the frequency of core damage in the past PRA's.

In order to illustrate one of the frontline systems models the generalized transient event sequence model is shown in Fig. 2.

Operator Actions

Dictated by the Bezau plant design, the operator actions play a vital role in many of the Bezau accident sequence analysis. Some of the operator actions are required as a part of the normal control of event sequences and others can be characterized as recovery actions to bring into function backup equipment when the normally responding equipment is not available. In total, the BERA risk model evaluates and quantifies over 60 different operator actions.
The quantitative assessment of a large number of diverse human responses, such as those modeled in BEIRA requires the achievement of two basic goals. The first goal is that it represents the state of the knowledge about human performance within the specified event scenarios. The second goal is that the operator action models must be internally consistent and externally benchmarked to achieve a degree of confidence in the results that is comparable to the system hardware analyses.

In order to achieve these goals, PLG decided not to apply an ivory tower approach to operator actions, but invited the Bezau operating staff to participate in the development of the basic input data for the operator action models. Five operator action evaluation parameters were defined, namely: Identification, Diagnosis, Decision, Response and Stress. Each of these were ranked on a relative scale of 1 to 10 for each operator action. From these, a difficulty index was calculated and a failure rate was then determined by locating benchmark operator actions within the difficulty index scale. Both the Bezau operating staff and the PLG staff independently completed the evaluation parameters for all operator actions. The basis for this quantitative evaluation was a documented qualitative evaluation of each operator action which included:

- Discussion of each specific scenario
- Time available for operator action
- Factors affecting operator response time
- Support system dependencies
- Significant preceding actions
- Procedural guidance
- Training and Experience
- Important features of operator response model

A large degree of consistency and agreement was observed in the independently evaluated difficulty indices between PLG and NOK. This provided confidence for the relative ranking of operator actions on a difficulty scale and the external benchmarking then provided the absolute scale for the operator action error rates. In some few instances notable differences between NOK's and PLG's assessment were observed. These were taken to indicate larger uncertainties in the operator action error rates.

3. RESULTS AND THEIR IMPACT ON BACKFIT DECISIONS

Comparisons have been made of the results of analysis for the different configurations and phases analyzed. The results of the phase A analysis indicated a number of plant features which dominated the possibility of core damage from internal events in a way which severely limited the benefit that could be potentially derived from the NANO backfit design. These limiting features included hardware, operating procedures and limitations of the Phase A model. The results of the Phase A analysis supported NOK decisions to implement a number of minor but effective improvements, many of which were already under consideration by NOK. The Phase A results have served to prioritize and accelerate decisions for the modifications listed in Table 1. The effect of these changes was investigated in the Phase A analysis. Results showed a significant improvement in the plant safety balance and a much greater effectiveness of the NANO backfit. Even the intermediate scope "Re-Re" backfit shows a significant improvement. In fact, the combination of these improvements with the "Re-Re" backfit is much more effective than the "PMU-NANO" backfit would be without the modifications of Table 1.

System importance rankings for the most highly contributing functions were estimated. The system importance ranking is expressed in terms of the proportional contribution to core damage which includes failure of the system function(s). Also estimated were the overall contributions which involved failure of specified functions. It was evident that in the Phase A analysis, failure of steam relief, failure of the operator to continue cooling with the unisolated steam generators when both steam generators have failed relief valves, and pressurized thermal shock failure of the pressure vessel during feed and bleed cooling, were represented in sequences which combined to account for more than half the total contributions to core damage. These weak points are all reflected in the modifications listed in Table 1. With these changes, the system importance ranking for Phase A results indicated a shift to failures in the auxiliary feedwater system, in establishing the bleed function for feed and bleed cooling, and in the recirculation cooling mode. For the "NANO-Re-Re" configuration it is interesting to note that recirculation failures contributed to 75% of the accidents.
The comparison of the three configurations investigated in Phase A of the "KWH-RERe" concept to be a well balanced design. Internal events and external events contribute about equally to the likelihood of core damage, and no one external event category dominates the contribution from the external events. The concept indicates a further "KWH-NANO" substantial reduction in the external event frequencies with a proportionately lesser reduction in the internal event frequency. For the "KWH-NANO" concept, internal events constitute 77% of the total.

The Phase A and AI portion of the Beznau PRA has helped to identify weak points which could be corrected with simple and inexpensive fixes. Many of these improvements were already under consideration internally at Beznau without the knowledge of the PRA team. The ability of the PRA to independently identify weak points already recognized or suspected by the operating staff has helped establish confidence in the PRA to indentify key plant weak points. The Phase A and AI portion of the PRA has also helped to identify and support a more cost effective backfit configuration which offers a balanced and adequate protection for both internal and external events. Phase B of the Beznau PRA is currently in the last phase of completion. Its major objective is to verify through a more complete and detailed analysis the findings of the Phase A analysis.

ACKNOWLEDGEMENT

The authors wish to thank Daniel W. Stillwell and John W. Stetkar of Pickard, Lowe and Garrick for their assistance in preparation of this paper.

<table>
<thead>
<tr>
<th>TABLE 1. DESIGN AND PROCEDURAL CHANGES FOR BERA PHASE AI - PLANT AS-IS CONFIGURATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. HARDWARE CHANGES</td>
</tr>
<tr>
<td>a. Steam generator relief valves (Ausblase Station). After a reactor trip:</td>
</tr>
<tr>
<td>(1) ARVs 1 through 3 stay in Tav mode but are not blocked unless reset by the operator.</td>
</tr>
<tr>
<td>(2) ARVs 4 and 5 automatically switch to pressure control.</td>
</tr>
<tr>
<td>(3) The setpoint for ARVs 4 and 5 will be below the steam generator safety valve setpoint.</td>
</tr>
<tr>
<td>(4) Drive motors will be upgraded.</td>
</tr>
<tr>
<td>b. New transformers for buses E and F with increased capacity.</td>
</tr>
<tr>
<td>c. The existing 8 kV and 6 kV transformers will be equipped with seismic wheel stops.</td>
</tr>
<tr>
<td>d. Add a fourth air compressor independent of PRN cooling as per NDK telex to PLG</td>
</tr>
<tr>
<td>2. PROCEDURAL CHANGES</td>
</tr>
<tr>
<td>a. Implement a procedure for 380V bus crosstie from bus K to bus H and from bus K to bus H.</td>
</tr>
<tr>
<td>for loss of offsite power sequences with the hydro station available in island service.</td>
</tr>
<tr>
<td>b. Implement a procedure to line up well water in the auxiliary cooling mode for cooling of the auxiliary feedwater pumps and plant air compressors if the 380V bus crosstie is not successful.</td>
</tr>
<tr>
<td>c. Insert a caution into procedure MV-K-1.1.5, &quot;Steam or Feedwater Line Break,&quot; to warn the operator not to isolate both steam generators if both steam generator safety valves are failed open, but feedwater is still available.</td>
</tr>
<tr>
<td>3. ANALYSIS CHANGES. Analyze pressurized thermal shock Top Event Y2.</td>
</tr>
</tbody>
</table>
TABLE 2  BEZNAU PLANT-SPECIFIC DATA COLLECTION SOURCES

Data Sources for Initiating Events, Component Failures, and Component Unavailabilities:

19,276 work requests (Arbeitssaufträge) examined for component failure occurrences.

9,408 tagout orders (Schaltaufträge) examined for component maintenance events and durations.

306 monthly operating reports examined for initiating events and plant power operating history.

344 special occurrence reports (Besondere Vorkommisse) examined for details of specific initiating events.

238 transmission line operation records examined for forced and scheduled outages (Phase B only).

59 quarterly operating reports examined for hydro Beznau operating history (Phase B only).

Data Sources for Success Data:

Component run time meters for pumps, compressors, ventilation units.

55 test procedures (Routine Vorschriften) examined for component operation demands and run times.

Plant power operating history.

Routine operating activities (startup, shutdowns).

Normal system operating configurations.

Technical specifications.

FIGURE 1. BERA PHASE A1 PLANT MODEL

<table>
<thead>
<tr>
<th>Phase A1 Model</th>
<th>ASIS</th>
<th>Hand</th>
<th>Kern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Sequences</td>
<td>$3 \times 10^6$</td>
<td>$1.8 \times 10^6$</td>
<td>$1.5 \times 10^6$</td>
</tr>
<tr>
<td>Number of End State Combinations</td>
<td>$1.7 \times 10^6$</td>
<td>$8.8 \times 10^6$</td>
<td>$8.8 \times 10^6$</td>
</tr>
</tbody>
</table>
USE OF PSA FOR RESEARCH REACTOR MANAGEMENT

SUMMARY OF PRESENTATION

Probabilistic Safety Assessment (PSA) is being applied to the Material Test Reactors at Harwell and associated major fissile loops. PSA has been used to support the revision of the safety documentation and also to check that plant modification and major experiments meet design safety criteria.

Improvements to refuelling plant and procedures have been made following PSA studies and examples of the application of PSA to a typical 10MW MTR were presented to the IAEA in March 1981. PSA has become an accepted tool in assessing the safety of major experiments in terms of risk to both workers and the public. The application of PSA has also highlighted possible adverse effects due to operator error and provided a logical approach to the study of Human Reliability. An important feature of the application of PSA to the Harwell MTRs has been to determine the sensitivity of top events to uncertain data and direct resources to improvements in plant and procedures.

H E CAMPBELL
SrD Culcheth
15 May 1986

Ref 1: F R Allen (et al). The application of probability analysis techniques to a typical 10 MW MTR. (Presented to the IAEA meeting on the presentation of a licensing guidebook for low enrichment research reactors, March 1981).
PLANT INFORMATION (PLUTO)

BUILT IN 1957

TANK TYPE, D2O COOLED AND MODERATED

OPERATES 25 DAYS AT 25 MW

SHUTDOWN 5 DAYS FOR REFUEL

AROUND 40 IRRADIATION EXPERIMENTS

MAJOR A.G.R. LOOP
THREE HAZARD GROUPS

EXAMPLE

1. REACTOR AT POWER
   LOSS OF COOLING

2. REACTOR SHUTDOWN
   REFUELLING

3. REACTOR EXPERIMENTS
   FISSILE LOOPS
OPERATIONS STAFF

SHIFT SUPERVISOR

SHIFT TECHNICIAN

2 CONTROL ROOM ASSISTANTS
P.S.A. (REFUELING)

EXAMPLES FROM STUDY

FUEL ELEMENT JAMMED

FAILURE OF GRAB TO SEAL

ELEMENT UNLOAD TO DRY HOLE

COMPRESSED AIR SUPPLIES

OPERATING INSTRUCTIONS

AVAILABILITY OF EMERGENCY SYSTEMS
Potential Operator Error
"Fuel Element Unloaded into Dry Hole"

1 x 10^-5
1.2 x 10^-8
7.66 x 10^-6
7.65 x 10^-6
7.1 x 10^-9
5.03 x 10^-3
5.5 x 10^-3
5.03 x 10^-3
1.1 x 10^-2
5 x 10^-6

5 x 10^-3
1 x 10^-6
1.2 x 10^-5
1 x 10^-3
1 x 10^-2
1. PREPARE FAULT TREE
2. DIMINISH THE DECEPTIONS
3. REWRITE UNCERTAIN DATA TO SEE EFFECT ON 'MEAN' 'MEANER' 'MEANINGLESS' - HUMAN ERROR VALUES - HARDWARE VALUES
4. SENSITIVITY ANALYSIS

PSA (EMERGENCY COOLING)

EXAMPLES FROM STUDIES
1. PROOF TESTING
2. INDICATIONS
3. EXACT RELIABILITY
   ISOLATION VALVES
   GAMMA MONITORS
   FANS
4. OPERATOR DEPENDANT ACTIONS
An investigation of ergonomic issues arising from a series of simulated LOCAs at DIDO and PLUTO reactors.

AIMS:

1) Determine whether the operators are able to bring the reactor to a safe and stable condition.

2) Determine whether there is any particular size or configuration of leak which proves especially difficult.

3) To determine whether operators use the same strategy to control a LOCA.
POTENTIAL ERGONOMIC PROBLEMS

1. Adverse environment within plant room
   Temperature, steam, spray, pressuriser
   suit, configuration of pipework.

2. Information overload.
   21 alarms within 90 seconds.

3. Lack of information.
   No bulk temperature alarm.

4. Task complexity.
   Calculation of leak rate.
SIMULATION EXERCISE

Information provided:
RAT level
SV level
D$_2$O bulk temperature
Alarms
Time

BENEFITS

1. Contribution to training
2. Additional assessment tool
3. Identification of inefficient strategies
4. Reveals ergonomic problems
5. Provides basis for modelling in PRA
CONCLUSIONS

1. SUPPORTS DETERMINISTIC ANALYSIS
2. NUMBER LESS IMPORTANT THAN IMPROVEMENT;
3. IDENTIFIES RELATIVE WEAKNESSES
4. ALLOWS SENSITIVITY ANALYSIS
5. PROVIDES BASIS FOR ALLOCATING RESOURCES
6. PINPOINTS DATA BASE REQUIREMENTS
7. CHECKS DESIGN TARGETS FOR EXPERIMENTS
   ARE APPROACHED
8. CONFIRMS AND HIGHLIGHTS NEED FOR
    DEPENDENT FAILURE ANALYSIS
    HUMAN FACTORS STUDY
Protection and segregation
Redundancy and voting (including maintenance time $\theta$
Proven design and standardisation
Derating and simplicity
Equipment diversity
Functional diversity

The choice of design options for a new plant or design change to an existing plant is determined by a number of factors:

- Cost
- Reliability
- Availability
- Maintainability

Consider the safety implications of a design. How do we differentiate between the benefits of a two or a four train design? What is the value of any form of barrier provided to segregate components or systems? How do we evaluate the effect of all defences applied in a particular design, and the cost/safety gains.

It should be possible to apply models of system unavailability, reliability and dependent failures in order to evaluate the benefits of any particular system configuration.

This note represents some speculation as to the problems and limitations of using probabilistic safety assessment techniques as evaluate tools.

Introduction

How do we evaluate the effect of the addition or removal of safety trains from redundant systems? If one train were removed from a four train redundant system what would be the effect on the system probability. Would it be adequate to simply remove the single train failure probability from the product of probabilities in a sequence, or is it necessary to consider interactions between individual channels.

Two methods of evaluating the impact of design changes are now discussed.

The date-free situation

Let us take as the starting point a list of defences which could be considered as necessary elements of a design in order to minimise the contribution of both independent and dependent failures to the overall system reliability (Table 2). If we wish to review a design for new plant at an early design stage then only a subset of these may be considered relevant.

<table>
<thead>
<tr>
<th>Table 1 New plant - defences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection</td>
</tr>
<tr>
<td>Redundancy</td>
</tr>
<tr>
<td>Design</td>
</tr>
<tr>
<td>Simplicity</td>
</tr>
<tr>
<td>Equip. Diversity</td>
</tr>
<tr>
<td>Func.</td>
</tr>
<tr>
<td>$0 &lt; m_k &lt; n_k &lt; 1.0$</td>
</tr>
<tr>
<td>$0 &lt; m_k &lt; n_k &lt; 1.0$</td>
</tr>
<tr>
<td>$0 &lt; m_k &lt; n_k &lt; 1.0$</td>
</tr>
<tr>
<td>$0 &lt; m_k &lt; n_k &lt; 1.0$</td>
</tr>
<tr>
<td>$0 &lt; m_k &lt; n_k &lt; 1.0$</td>
</tr>
<tr>
<td>$0 \leq \beta \leq 1$</td>
</tr>
</tbody>
</table>

From the above analysis an overall $\beta$ factor can be derived such that $\beta = \prod_k m_k$ can be evaluated in terms of the $m_k$ for each competing system $K$.

The minimum values, $m_k$, are in effect weighting factors measuring the relative beneficial effect of defence $K$. The assessed factors, $n_k$, reflect the judged quality of each defence in a given design. Since it lies in the interval $[0,1]$, $m_k$ may be interpreted as the probability of a single channel failure being a dependent failure if defence $K$ applied alone. If a sufficient dependent failure events database is accessible, the $m_k$ may be estimated empirically; otherwise they will have to be calibrated by subjective judgement. SBD experience is that a factor $0.8$ or $0.7$ is reasonable for many designs. The reader is referred to the published statements of $\beta$ values in the literature. The factor $0.8$ or $0.7$ is often quoted as a reasonable value for $\beta$.

It is especially important to note the designed system configuration during m'tcs and test operations e.g., does a 2oo3 system logic become 2oo2 or 2oo1?
is obtained. This value characterises the effectiveness of the defensive strategy for the system, and is to be compared with the $\beta$ values of competing system designs.

**Example Application**

Consider now the two systems shown in Fig. 1. System design no. 1 comprises of two channels performing the same function but using different components visi- $\square$, $\Delta$. There is also a low quality barrier between the two channels. Conversely, system design 2 comprises of four identical channels, performing the same functions and using identical components $\square$, $\Delta$. There is also a high quality barrier between each channel.

**System design 1**

```
Channel 1

Channel 2
```

**System design 2**

```
Channel 1

Channel 2

Channel 3

Channel 4
```

**Competing design evaluation**

The two system designs are compared using the list of defences given in Table 1, and a value $x_k$ is assigned to each system defence. For the two systems under consideration the result would be:

$\beta(1) \geq x_k(2)$

$\beta(1) \geq x_k(2)$

$\beta(1) \leq x_k(2)$

$\beta(1) \leq x_k(2)$

$\beta(1) = x_k(2) = 1$

The situation where data exists

When generic dependant event data is available another technique known as the impact vector assessment method can give a guide to decision-making of the type discussed in this paper. This is essentially a data-screening technique, and consequently the caveats which apply to data screening also apply to this method. However, if data are screened consistently the technique may serve to evaluate system design in a relative sense. The basic idea of the method is shown in Fig. 2.

![Fig 2](image_url)

**It is the screening for applicability which entails the use of impact vectors:**

<table>
<thead>
<tr>
<th>Event No.</th>
<th>XYZ</th>
</tr>
</thead>
<tbody>
<tr>
<td>P0</td>
<td>0</td>
</tr>
<tr>
<td>P1</td>
<td>0</td>
</tr>
<tr>
<td>P2</td>
<td>0</td>
</tr>
<tr>
<td>P3</td>
<td>0</td>
</tr>
<tr>
<td>P4</td>
<td>0</td>
</tr>
<tr>
<td>N/A</td>
<td>0</td>
</tr>
</tbody>
</table>

- **System 1**
- **System 2**

**Fig. 3 - Example of impact vector**

The entries in the impact vector are obtained by judgements on the part of the data analyst/decision-maker. The entry for each respective system under $P_k$ is the (subjective) probability that $k$ redundancies would be affected in system if event no. $x_k$ occurred in that system. Depending on the analyst's assessment of the defences built-in to the competing designs, events which are applicable to one system may not be applicable to another system design, thus better designs of system may be identified. Formally, the system with best defences will have fewer dependent failure events judged to be applicable to it, and consequently $\beta$ values estimated from such impact vectors (one for each event in the generic database) will be minimised for that system.

$\beta$ Although no use is made of the fact here, $\beta$ as derived here may be used in Fleming's $\beta$ factor model, hence the notation.

$\beta$ If in the database a fire occurred in a 3 channel system which was adequately segregated and hence affected all 3 trains, this event would be judged to affect 1 channel of system 2 only because of good segregation hence $P_2 = 1$, while $P_1, P_3, P_4 = 0$. 

3 4
Summary

Two methods have been outlined which may usefully serve as a guide to management at the early design stage. By careful selection of a further subset of defences from Table 2, the techniques discussed here could also be applied to the evaluation of the impact of design changes in existing plant.

Design control
Design review
Functional diversity
Equipment diversity
Fail-safe design
Operational interfaces
Protection and segregation
Redundancy and voting
Proven design and standardisation
Derating & Simplicity
Construction control
Testing and commissioning
Inspection
Construction Standards
Operational control
Reliability monitoring
Maintenance
Proof Test
Operations

Table 2 System Defences
Probabilistic Safety Assessment as an Aid to Nuclear Power Plant Management

Session 4
Introductory Paper

Which Risk-Related Quantities Should be Managed?

N J Holloway

Contents

1. Introduction - Possible Forms of Expression of Risk
2. Actuarial Considerations
3. Capabilities and Costs of Risk Analysis
4. Possible Quantities and Equations
5. Conclusions

References

Safety & Reliability Directorate
U K Atomic Energy Authority
Colneheath, Warrington, WA3 4NE.

May 1986
1. INTRODUCTION - POSSIBLE FORMS OF EXPRESSION OF RISK

The management of risk requires that it be expressed in quantitative forms, so that increases and reductions can be estimated as functions of management policies and actions.

The past practices of risk assessment have established the use of various forms of risk expression, some more quantitative than others, and some relating more directly than others to measures of harm to people.

Amongst the direct, quantitative forms of risk expression, we may count the following as well established in past practice:

1) Frequency/consequence graphs relating to the frequency of occurrence of accidents resulting in a particular consequence or worse (P-W lines).
   Consequences of early death, delayed death, injuries, loss of food production, loss of land use etc. have been expressed in this form in many risk assessments.

2) Individual risk estimates, relating to early or delayed death, or injury.

Amongst the indirect expressions commonly used, we may count:

3) Core melt frequency
4) Frequency of 'beyond design basis accidents'
5) Frequency of 'uncontrolled releases'

These expressions, while certainly connected with risks, do not allow immediate assessments of harm to people, although immediate assessment of certain upper limits on such quantities may be made.

At a further remove from risk, deterministic assessments related to regulations for design and operation are to be found. Some of these are used in the construction and operation of all nuclear power reactors, but probabilistic analysis suggests that conformance to these deterministic regulations does not by itself relate strongly to quantitative risks.

ACTUARIAL CONSIDERATIONS

The existence of a variety of possible undesirable consequences, and hence risks, from nuclear power plant operation, can lead to difficulty in management of risks and resources, if the risks of various types have to be treated separately, with incompatible measures. Evaluation of trade-offs and risk reduction priorities in this 'vector' (i.e. multi-component) situation can prove impossible without some common basis for evaluation.

This leads naturally to the search for a common basis within which to evaluate risks and expenditures of resources to prevent them. Several possible concepts could be used, but since money was (presumably) invented for the purpose of expressing and trading varied resources, it is the natural choice for a common basis. Since we have developed 'actuarial' approaches to many aspects of society's activities, in order to relate and prioritise them, it is natural to adopt an actuarial approach to the evaluation of risks and resources in nuclear power plant operations.

Actuarial assessments of plant damage in nuclear power plants present no great problems, particularly since the accident at Three Mile Island has given us an example of serious plant damage almost completely independent from any human health effects. The fact that serious plant damage costs are very high and relatively easy to assess provides a promising start to an actuarial approach to safety management in respect of severe accident avoidance.

Much more difficult is the actuarial assessment of health effects. Although such assessments are common in many industries, either in deliberate calculation or by default in policy decisions, quantitative values differ by orders of magnitude. Within the nuclear industry, some effective life evaluations are used in low dose radiation protection, although even here there are inconsistencies in values.

Despite these difficulties, health effect evaluations in financial terms are not likely to be any less accurate than the estimations of health effects which probabilistic studies produce, and there is no obvious reason why they should not be used, provided that the uncertainties (possible ranges of values) are recognised. A previous study (Ref 1) which compares the plant and offsite effects mentioned above based on past risk studies, uses some health effect actuarial evaluations as suggested, together with some evaluations for effects such as loss of land/building use which must rank as intermediate between direct plant losses and health effects in their difficulty of evaluation.

Actuarial approaches to the assessment of risks and costs in a scalar measure present us with a possible mechanism for optimisation according to the ALARA principle. They apply most easily to the on-site, plant losses which would arise in severe (risk dominant) accidents, and (as suggested in the reference and in later sections of this paper) these may well be the dominant losses in such accidents. This dominance reduces the importance of some of the difficulties of applying actuarial methods to life and health evaluations.

3. CAPABILITIES AND COSTS OF RISK ANALYSIS

The operation of the ALARA principle, in respect of severe accident risks, depends upon the capability of our methods to analyse risks. Furthermore, the costs of the analysis itself may become significant in the optimisation process.

Although the capability of probabilistic assessment is frequently questioned, on the basis of the lack of relevant experience and the uncertainties introduced, this capability has been improving rapidly, and it is not unreasonable to plan in terms of somewhat better performance than we now observe. Furthermore, the critic-
issue of PRA should be seen in the context that no serious alternative method of assessing the risks quantitatively has yet emerged.

The cumulative nature of the PRA process is such that uncertainties in numerical results increase as the stages of accidents proceed in the analysis. Within the severe accident risk estimation process, these uncertainties increase as one goes through the following stages:

i) Beyond design basis accidents  
ii) Core meltdown accidents  
iii) Serious releases from containment  
v) Offsite health effects  
vii) Assessments of other social/political effects of severe accidents

From this point of view, the nearer to the top of the list one can make the necessary assessments for risk management, the better in terms of uncertainty, and the lower the costs of the analysis.

Core meltdown stands out as one obvious point of assessment. It involves a high and relatively accurately known cost of plant loss, not necessarily typical of all beyond design basis accidents (for example, a Small LOCA with leaking containment is beyond design basis in the UK, but would not do much damage to a PWR plant). Assessments of core meltdown frequencies continue to have significant uncertainties, but these are usefully limited by historical experience, and seem to be approaching the necessary accuracy for plant management over a wide range of accident issues.

However, analysis beyond core meltdown introduces further costs of analysis and unavoidable uncertainties, it is not possible to escape it altogether in a risk management scheme, as only the serious releases are important in the dominant public perception of reactor accidents. They seem to be numerically dominant in risk in most past PRA studies as well, perhaps indicating that at least this part of public perception has some sense to it.

However, it may well be unnecessary to utilise the full capabilities of plant and site specific PRA in order to incorporate post-core-melt assessment into a management scheme. Sufficient information on the behaviour of PWR containments following specific accident sequences, and on the risks to the public imposed by characteristic large releases, is already available from previous studies, and for a new plant and site, with no particularly novel containment or site features, a simple model based on past studies may be sufficient. Such a model would already draw upon the full capabilities of PRA, and could draw upon a limited amount of plant specific analysis if such were required. It appears likely that the uncertainties in using simplified approaches would add little to the uncertainties which arise from difficult generic issues such as source term mitigation and NPP.

The costs of setting up a PRA model to the stage of core melt, plus some simplified treatments of post-core-melt releases and consequences, would probably amount to about one half the typical costs of a historic PRA, which implies some one million dollars cost or so. This sort of figure could be used in any early assessments of the costs of setting up a scheme, to be added to the costs of operating it in the plant management process. The latter costs would be highly sensitive to the level of detail and frequency of use of the model. Initial costs could of course be spread over a programme of more than one similar reactor plant.

4. POSSIBLE QUANTITIES AND EQUATIONS

The foregoing considerations suggest that some form of risk management could be based on the core melt frequency as one important component in the 'managed quantities', with some further quantities relating to the particular core melt accidents which give rise to enhanced probability of containment failure and serious offsite effects.

Reference 1 provides some analysis of past PRA's which indicates the way in which core melts divide into release classes and associated consequences. Only the major releases of activity lead to total accidental losses well above the level of losses on the plant itself, while the core melts with minor releases from an essentially intact containment lead to little loss other than that of the plant.

Historic PRA's suggest that core melt accident sequences, identified at the system level, and prior to delineation of phenomenology of molten cores, can be crudely divided up as follows:

i) Core melt accidents in which containment cooling systems are available and no bypass occurs, lead normally to very small releases, with only a small probability (circa 1% or less) of major containment failure and activity release.

ii) Core melt accidents in which the containment cooling systems also fail, or in which the containment is bypassed, lead to major releases, and serious offsite effects.

According to this understanding of core melt sequences, a crude scheme for assessing the risk from a spectrum of core melts allocates the containment cooling failure and bypass sequences to high offsite consequence categories, together with a small percentage of the other core melts. The remaining core melt sequences are left in a negligible offsite consequence category.

The number of high offsite consequence categories required for this scheme is of course open to choice. Historic PRA's suggest that the following categories
of sequences in a large dry PWR design would be worth approximate evaluation and use in a simple consequence assessment scheme:

i) Interfacing LOCA (VASH-1400 "W" sequence)

ii) Core melt following SG tube rupture

iii) Core melt with failed containment cooling (delayed failure)

iv) Core melt with early containment failure.

The last simply being a recognition of various low probability catastrophic failure modes attributable to steam explosions, hydrogen burns etc.

Actuarial evaluation of these consequences could be done with methods such as those suggested in reference 1. This would lead to a list of core melt categories with associated onsite and offsite actuarial losses, and an overall actuarial loss expectation made up as follows:

\[ \text{Total expected actuarial loss} = \sum \left( f(\text{cat}_i)( c + c_i) \right) \]

where \( i \) labels the core melt sequence category, \( c \) is the cost of a core melt on the plant (approximately the same for all core melts) and \( c_i \) is the actuarial loss attributable to the expected offsite effects for the core melt sequence category. For core melts without bypass or containment cooling failure, \( c_i \) would be approximately given by:

\[ c_i = P_{\text{ef}} c_{\text{ef}} \]

where \( P_{\text{ef}} \) = probability of early containment failure for a core melt

\[ c_{\text{ef}} = \text{offsite losses for an early containment failure} \]

(It is expected that the product \( P_{\text{ef}} c_{\text{ef}} \) would be small compared with the plant loss cost \( c \)).

Reference 1 compares the likely values of the contributors in an equation of the above type, for the total actuarial losses in core melt accidents. On the basis of past studies, the contribution from onsite losses appears likely to be larger than that from offsite losses. Thus, to a large extent, the uncertainties associated with offsite effect calculations are "diluted" by the presence of a large and relatively much more certain contribution to the total. This is an important and encouraging feature of the actuarial loss assessments, helping to justify the necessarily crude models suggested for the offsite assessments in the scheme.

(Note: In reference 1, accidents which write off the plant but do not cause core melt or major releases are also considered. Past studies have not in general attempted accurate assessments of these accidents' frequencies, but have often used conservative or limiting values. The high contribution to actuarial losses from such accidents may merit a more serious assessment, but this is not addressed in any further detail here.)

5. CONCLUSIONS

Preliminary assessment of the possibilities for approximate evaluations of losses associated with severe accidents suggest that risk-related quantities, estimated at the stage of core melt sequence quantification in a PRA, may be useful and appropriate in a risk management scheme. Such a scheme could be based upon a selection of 'once-off' calculations for post-core-melt behaviour, or, more cheaply, upon deductions and extrapolations from the many existing PRA results. Risk assessment in such a scheme would apply actuarial losses to accident sequences, according to their propensity to lead to serious releases of activity, rather than according to fully detailed post-core-melt analysis for all sequences.

A scheme based upon evaluation of losses (actual and prospective) at the core melt sequence stage would be intermediate between many current risk management schemes, which evaluate the possibilities of exceeding a design basis, and schemes based on fully detailed consequence analysis (full PRA). The way in which the intermediate scheme would add extra weight to accident sequences likely to give large releases would naturally result in additional aversion of such accidents relative to contained core melts. This would reflect both increased public concern with large releases and conformance to a 'cliff edge' principle which has been used in the UK to express the same idea that the large release accidents should be significantly less likely than the total of beyond design basis accidents.

References

This paper is an appendix to "Which risk-related quantities should be managed?"; it was distributed but not presented orally at the Workshop.

Foreword

This short paper addresses the relative actuarial costs of onsite and offsite effects in severe PWR accidents. Particular reference is made to the results of the Sizewell B probabilistic safety study, as presented to the UK Public Inquiry via the CEGB's Proof of Evidence 16. The results of some comparable studies of reactors in the United States, Sweden, and West Germany are also considered and compared.

Summary

Onsite costs are found to dominate offsite costs for core melt accidents, under most of the plausible variations of the comparisons. This result is especially true for the Sizewell B plant at the proposed site. The result allows a simple actuarial assessment equation for severe accidents to be set up, based on level 1 (core melt) assessments rather than on level 3 (offsite effects) assessments, once example level 3 assessments have been done.

Contents

1. INTRODUCTION
2. A SURVEY OF DEGRADED CORE ACCIDENTS FROM VARIOUS PROBABILISTIC ANALYSES OF PWR's
3. ASSESSMENT OF ECONOMIC LOSSES IN DEGRADED CORE ACCIDENTS
4. ACTUARIAL ASSESSMENT OF DEGRADED CORE RISKS
   4.1 Simple Approximations to Actuarial Assessments
5. CONCLUSIONS

References

Tables 1-3
INTRODUCTION

The management of safety in UK nuclear power plants makes use of the ALARP (As Low As Reasonably Practicable) concept with respect to risks emanating from plant operations. Although the interpretation of the word Practicable does not fully imply an equivalence with cost-benefit analysis, it has some aspects in common with that discipline, one of which is a need to quantify risks and costs of avoiding them in some common valuation.

The present paper discusses quantification of the risks from NPP operation, and particularly the relationship of risk quantifications for onsite (plant) losses and offsite (health and societal disruption) losses. Some risk study results are used to illustrate possible quantifications, and to compare onsite and offsite losses for typical large dry PWR accident 'spectra'. Foremost amongst the risk studies is the Sizewell B probabilistic safety study, in the form presented to the Public Inquiry through CEGB Proof of Evidence 16.

A SURVEY OF DEGRADED CORE ACCIDENTS FROM VARIOUS PROBABILISTIC ANALYSES OF PWR's

There are now many probabilistic safety studies completed for PWR plants with large dry containments. As examples, we take the following studies, which emanate from different countries and refer to different reactor vendors.

<table>
<thead>
<tr>
<th>Country</th>
<th>Safety Study / Reactor</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK</td>
<td>Sizewell PSS / Sizewell B</td>
</tr>
<tr>
<td>USA</td>
<td>WASH-1400 / Surry 1</td>
</tr>
<tr>
<td>USA</td>
<td>Oconee PRA / Oconee 3</td>
</tr>
<tr>
<td>FRG</td>
<td>German Risk Study phase A/ Biblis B</td>
</tr>
<tr>
<td>Sweden</td>
<td>Ringhals 2 PSS</td>
</tr>
</tbody>
</table>

Of these, only the last does not analyse containment responses and activity releases, and for the purposes of comparison, releases are assessed for Ringhals by drawing parallels with similar accident sequences in the other studies.

External hazards are only assessed in detail in the Oconee PRA. These are eliminated from the Oconee results for the purposes of the present study.

The survey of the degraded core accidents from the probabilistic studies is based upon identifications of the following types of accidents (in decreasing order of severity)

<table>
<thead>
<tr>
<th>Severity level</th>
<th>Types of accident</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Core melt with major early failure of containment. Includes interfacing LOCA and early overpressure or steam explosion failure, and failure to isolate.</td>
</tr>
<tr>
<td>2</td>
<td>Core melt with delayed failure of containment or early failure with significant mitigation of release. Includes core melt with loss of containment cooling.</td>
</tr>
<tr>
<td>3</td>
<td>Core melt with only minor leakage of containment and no above ground failure. Includes basement failures.</td>
</tr>
<tr>
<td>4</td>
<td>Accidents with no core melt, but probable plant write-off. Includes major LOCA's.</td>
</tr>
</tbody>
</table>

Activity releases from these accident classes have been variously estimated in the studies, but there are sufficient similarities within each category to justify the use of 'generic' releases. These releases, and the offsite effects resulting from them, are standardized to the Sizewell B releases as follows:

<table>
<thead>
<tr>
<th>Severity level</th>
<th>Appropriate Sizewell PSS release</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UK 1</td>
</tr>
<tr>
<td>2</td>
<td>UK 5</td>
</tr>
<tr>
<td>3</td>
<td>UK 11</td>
</tr>
<tr>
<td>4</td>
<td>UK 12</td>
</tr>
</tbody>
</table>

The approximate frequencies in each severity level from the selected studies are listed in Table 1. Some of the release categories in the original studies have been re-interpreted to accord with the distinct severity levels above - for example, the WASH-1400 overpressure failures have been put in severity level 2, where later analysis suggests they should be, although in WASH-1400 they were
in the same category as interfacing LOCAs. Core melts with steam
generator tube breaks, leading to containment bypass, are treated
as severity level 1, although some studies place these in a lower
release category than the interfacing LOCA. Both types of contain-
ment bypass accident are currently subject to intensive investigation
with respect to the magnitude of the release. We consider both the
traditional large releases and the possibilities of much reduced
releases.

3. ASSESSMENT OF ECONOMIC LOSSES IN DEGRADED CORE ACCIDENTS

In this section we consider the probable economic losses in
degraded core accidents, making use of the Sizewell B study on its
specific UK site as an indicator of offsite losses. Only the direct
losses, including plant and life losses, and direct economic disruption,
are considered here. In an appendix, ' Programme Losses ' which
may arise from changes to related reactor programmes are also con-
idered, but it is there suggested that these should not be considered
on the same footing as the direct losses.

The onsite losses in a degraded core accident are relatively
easy to quantify. Slightly used plants have a typical value of
£ 1 x 10^9, and the TMI degraded core accident suggests that cleanup
costs etc can increase this loss by a factor of 2 or 3. Accidents
emanating from large LOCAs which lead to only slightly degraded
core conditions also have a large economic loss, of order £ 1 x 10^9,
but less associated cleanup costs. Thus the direct costs onsite
of degraded core accidents and large LOCAs are estimated to be:

- Core melt: £ 2 - 3 x 10^9
- L LOCA: £ 1 x 10^9

Offsite losses are much more difficult to quantify, particularly
when large releases are involved. The most serious losses are the
losses of life, and a life evaluation must be used to assess these
on a basis comparable with onsite costs. Life evaluations are now
routine in radiological protection against low dose ( cancer ) effects
and amount to between one and ten million US$ in most cases. Early
deaths have not been evaluated to the same extent, but clearly
require a higher valuation. For the purposes of this paper, the
following valuations are used:

- Early death: £ 10^7 ( x. / 3 )
- Delayed: £ 10^6 ( x. / 3 )

and, in ' inflation proof ' terms, this can be thought of as:

One plant value = 100 life values ( early death ) = 1000 " ( delayed " )
(with error factors of 3 either way)

Other offsite losses are more easily considered in economic
terms. The principal losses are interdiction of land and dwellings
and loss of foodstuffs, over fairly long periods of time. Short term
emergency actions tend to have lower economic impacts than the long
term actions, even though the short term actions may affect more
people and larger areas.

Long term economic losses, assessed on the basis of the Sizewell
consequence calculations, can be roughly assessed on the basis of
the numbers of people relocated for long periods ( or indefinitely ).
All the economic investments associated with those people - their
industries, homes, land etc, can be reasonably assumed ' lost ' in
the relocation. Thus the assessment depends only on the average
economic investment value associated with a member of the population.
Since economic activity is typically 5% to 15% of investment per year,
we can estimate the investment as about 10 times per capita GNP, or,
in the UK, some £ 40,000.

This will overestimate the mean losses on relocation because
some of the investments associated with a person's economic activity
are transportable - for example, education, most forms of documented
knowledge, monetary investments etc. This overestimation compensates
for the neglect of some other costs, such as the relocation itself,
and the costs of avoiding activity in the interdicted areas ( re-routing
of roads etc).

The above simple models for assessing the impacts offsite in
severe releases, can be used in conjunction with the Sizewell assess-
ments of damage for releases UK 1, UK 5, UK 11, and UK 12. The
results of this are tabulated in Table 2. The Sizewell assessment
evacuated population is assumed to be the same as the relocated pop-
ulation, in accordance with the model used. Later assessments have
suggested that the numbers relocated to avoid long term groundshale
may be somewhat larger, but not enough to upset the basic relativi-
ties of the simple models being used.

Table 2 figures, even for the first estimate ( conservative )
consequences in the Sizewell B assessments, show that the offsite
losses only marginally exceed those onsite in the cases of the
large releases, and that they are trivial in the cases of the small releases (severities 3 and 4). Inclusion of other health effects such as non-fatal thyroid cancer does not significantly affect these conclusions, neither do the suggested uncertainties in the evaluations, except that downward revisions of the source terms, coupled with lower cost evaluations, could make even the larger release impacts offsite smaller than those onsite.

The only change in circumstances which would make the offsite impact of the larger releases much greater than the onsite impact would be siting in a high population area. Comparative studies for different UK reactor sites suggest that some sites would produce about three times the Sizewell expectation numbers of casualties, relocations etc. On such sites, the offsite impacts could approach ten times the onsite impacts for the largest releases (using conservative release magnitudes, such as the First Estimates).

ACTUARIAL ASSESSMENT OF DEGRADED CORE RISKS

We can use the simple estimates of post-accident economic impacts of core melt accidents, together with the core melt frequencies (section 2 and Table 1) from the PRA's, to assess roughly the relativity of risks from various types of accident sequence. The results, produced by multiplying accident frequencies from Table 1 with impacts from Table 2, are tabulated in Table 3. An onsite impact of $2 \times 10^5$ for core melt, and $1 \times 10^5$ for L LOCA is used. First estimate source term impacts from Table 2 are used. Use of the second estimate source terms from Table 2 would reduce the offsite values in Table 3 by about a factor of 4, while leaving the onsite values unchanged.

An inspection of Table 3 reveals the following:

i) Onsite impacts for core melt accidents tend to dominate offsite impacts, even for the conservative first estimate source terms. This is particularly true for Sizewell B, and only marginally untrue for Biblis B, partly as a result of the categorization of all Biblis core melts as at least delayed overpressure failures. Use of the Biblis source terms instead of the general severity level 2 source term would reverse the dominance, as would use of the second estimate source terms.

ii) The onsite impacts of core melts for Sizewell B are sufficiently dominant that they would continue to be so on a more populous UK site, especially if reduced source terms are used.

iii) The costs associated with Large LOCA are generally high compared with the costs associated with core melts. This is especially true for Sizewell B. This dominance may be quite artificial, and results from the fact that the PRAs have assessed large LOCA frequencies to be as high as is reasonably possible without conflicting with the non-occurrence data over a thousand reactor years of operation. Detailed fracture assessment for large LOCA could well reveal expected frequencies orders of magnitude smaller. Thus the Large LOCA assessments cannot be taken as strictly comparable to the core melt assessments.

iv) The 'post-PRA' Sizewell design shows two clearly beneficial features in comparison with the 'pre-PRA' designs of the other reactors, i.e.:

a) A significantly lower core melt frequency
b) A significantly better risk profile - in that the more severe releases are avoided to a greater degree.

Together, these produce a very large reduction on the assessed offsite impacts for Sizewell, so that the marginally lower offsite impacts typical of the other reactors have become substantially lower for Sizewell.

The extent to which the better risk profile of Sizewell B can be attributed to the PRA process is open to debate. However, it is clear that PRA has highlighted the possibility for some types of core melt accident to release much more than others, and that such types are particularly suppressed in the Sizewell design, relative to older designs in which this distinction amongst different severe accidents was less well recognised.

4.1 Simple Approximations to Actuarial Assessments

Because it is apparent that offsite impacts, even with their associated uncertainties, are not likely to dominate over the more certain onsite impacts of severe accidents, simple approximations for the overall risk impacts of severe accidents are plausible.

The basis for one such simple approximation is as follows:
1) Accidents writing off the plant can be assessed as involving one unit of loss, approximately equal to the value of a 'slightly used' PWR, currently some £1 x 10^8. This loss is simply associated with the plant loss and should be added to any further losses.

2) Accidents involving core meltdown, but with fairly effective containment of activity, can be assessed as involving a further unit of loss, additional to the plant write-off cost of one unit. This covers cleanup costs etc, for which TMI-2 has provided an example. The small activity releases have negligible offsite costs in comparison.

3) Accidents involving serious containment failures or bypass, following a core melt, can be assessed as producing some 1-10 additional units of cost. The lower end of this range would be appropriate to remote sites and the higher end appropriate to populous sites. Confirmation of reduced source terms for these severe releases would reduce the associated costs roughly in proportion.

This simple model provides an 'Actuarial Risk Equation' for severe accidents as follows:

\[
\text{Risk} = 1 \times \text{plant write-off accidents (no core melt)} + 2 \times \text{core melts} + \times \text{severe releases.}
\]

where \( \times \) is between 1 and 10 depending on type of site. For Sizewell r would be about 4^2. The unit of the risk equation would be a plant value, per whatever time period was selected (eg 1 year or the plant lifetime).

(* Nearer to 1 for second estimate source terms *)

5. CONCLUSIONS

The study of some past risk assessments, with particular emphasis on the Sizewell B Probabilistic Safety Study, suggests that the overall economic impacts of severe PWR accidents, including reasonable evaluations for the health effects of severe releases, are dominated by onsite losses, rather than the losses associated with releases of activity to the environment. The dominance of onsite losses is particularly great if non-core-melt accidents such as the Large LOCA are assumed to occur with frequencies greater than the frequencies of core melt accidents.

Because the onsite economic losses due to core melt or other major damage to plant are relatively certain, it is possible to construct quite simple actuarial assessments for the expected total economic impacts of onsite and offsite damage. The relatively large uncertainties in assessments of offsite losses alone are 'diluted' by the additions of larger and more certain contributions to the total. For reactors such as Sizewell B, which are on fairly remote sites, and which have a small probability of major releases following a core melt, the use of a simple actuarial assessment is particularly effective.

The use of a simple assessment scheme, based on the identification of basic types of core melt sequences, rather than on detailed post-core-melt analysis, could be implemented once an example assessment (such as the Sizewell PSS) had been performed, allowing the offsite losses for core melt types to be estimated. Repetition of the post-core-melt analysis would not be necessary within the risk management scheme based upon it.

The use of a risk management scheme based upon a simple actuarial assessment would be expected to result in the following trends in the expected frequencies of severe accidents:

1) Core melt accidents would be avoided to the extent determined by guidelines for the frequencies of accidents beyond the design basis.

2) The specific core melt accidents with a propensity to major releases (eg containment bypass accidents) would be avoided to a greater degree than the general class of beyond design basis accidents.

3) Design basis accidents with plant write-off outcomes would be avoided to the extent of economic optimum levels.

(Probably in the 10^-5 to 10^-3 per year range)
These outcomes of the application of an actuarially based risk management scheme would automatically conform to the concept of avoiding a 'cliff edge' effect just outside the design basis, as additional aversion measures would be applied to the accidents with particularly large offsite consequences. It might also have some influence on matters of protecting plant against serious damage in design basis accidents, although there is already quite a high level of protection against this.

**References**

References are to the PRA documents for the five reactors considered. Sizewell B PSS results are taken from CEGB Proof of Evidence 16, and the associated NRPB Report 137.

### Table 1

**ACCIDENT FREQUENCIES BY SEVERITY LEVELS FROM SELECTED PSS's**

<table>
<thead>
<tr>
<th>PSS</th>
<th>Frequencies in severity levels ($10^6$ yr)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Sizewell</td>
<td>0.046</td>
</tr>
<tr>
<td>WASH-1400</td>
<td>16*</td>
</tr>
<tr>
<td>Oconee 3</td>
<td>0.65</td>
</tr>
<tr>
<td>Biblis B</td>
<td>2.6</td>
</tr>
<tr>
<td>Ringhals 2</td>
<td>1.0</td>
</tr>
</tbody>
</table>

**Notes**

* In order to produce compatibility with other studies, the WASH-1400 median values have been converted to mean values using the stated error factors. For the severity categories 1 and 2 this results in an increase by a factor of 2.7.

* Much of this is Oconee category 4 release, which is a very late overpressure (60 hours after initiating event) and which is estimated to give a lower release than the Sizewell UK 5 release.

+ It is difficult to assign this quantity from the Ringhals study, which did not consider containment failures other than bypasses. The number has been derived from sequences resulting from loss of AC power or large LOCA with spray failure (results in containment failure)

( ) around severity 4 frequencies: None of these frequencies have been derived as best estimates, but have relied mainly on the non-occurrence data. Use of up to date non-occurrence data would reduce the 1000 values to less than 500 in 1985.
OFFSITE IMPACT ASSESSMENTS FOR SIZEWELL B RELEASES
FIRST ESTIMATES

<table>
<thead>
<tr>
<th>Release Category</th>
<th>Severity Level</th>
<th>Consequences / Assessments</th>
<th>Total Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Deaths Early</td>
<td>Late</td>
</tr>
<tr>
<td>UK 1</td>
<td>1</td>
<td>130</td>
<td>3300</td>
</tr>
<tr>
<td>UK 5</td>
<td>2</td>
<td>12</td>
<td>2200</td>
</tr>
<tr>
<td>UK 11</td>
<td>3</td>
<td>0</td>
<td>1.4</td>
</tr>
<tr>
<td>UK 12</td>
<td>4</td>
<td>0</td>
<td>0.44</td>
</tr>
</tbody>
</table>

Notes
* Many of these are precautionary evacuations and would not imply long term relocation. Thus the associated costs are overestimated.

SECOND ESTIMATES

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UK 1</td>
<td>1</td>
<td>4.8</td>
<td>1300</td>
<td>3600</td>
</tr>
<tr>
<td>UK 5</td>
<td>2</td>
<td>0.6</td>
<td>560</td>
<td>2400</td>
</tr>
<tr>
<td>UK 11</td>
<td>3</td>
<td>Not distinguished from</td>
<td>0.04 \times 10^8</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UK 12</td>
<td>4</td>
<td>the first estimates</td>
<td>0.04 \times 10^9</td>
<td></td>
</tr>
</tbody>
</table>

ACTUARIAL ESTIMATES OF RISKS ASSOCIATED WITH ACCIDENTS OF THE SELECTED SEVERITY LEVELS

( Figures are based on First Estimate values from Table 2 )

TABLE 3A: ABSOLUTE VALUES FROM EACH PRA

<table>
<thead>
<tr>
<th>Reactor/PSS</th>
<th>Onsite</th>
<th>Offsite</th>
<th>Impacts by severity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Sizewell B /</td>
<td>92</td>
<td>20</td>
<td>2360</td>
</tr>
<tr>
<td>Sizewell PSS</td>
<td>258</td>
<td>30</td>
<td>47</td>
</tr>
<tr>
<td>Surry 1 / WASH-1400</td>
<td>32000</td>
<td>32000</td>
<td>136000</td>
</tr>
<tr>
<td></td>
<td>89600</td>
<td>48000</td>
<td>2720</td>
</tr>
<tr>
<td>Ocone 3 PRA</td>
<td>1300</td>
<td>22000</td>
<td>84000</td>
</tr>
<tr>
<td></td>
<td>3640</td>
<td>33000</td>
<td>1680</td>
</tr>
<tr>
<td>Biblis B / GRS</td>
<td>5200</td>
<td>154000</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>14560</td>
<td>231000</td>
<td>-</td>
</tr>
<tr>
<td>Ringhals 2 PSS</td>
<td>2000</td>
<td>400</td>
<td>7600</td>
</tr>
<tr>
<td></td>
<td>5600</td>
<td>600</td>
<td>152</td>
</tr>
</tbody>
</table>

TABLE 3B: FRACTIONS OF TOTALS FOR CORE MELTS

<table>
<thead>
<tr>
<th></th>
<th>0.03</th>
<th>0.007</th>
<th>0.84</th>
<th>0.88</th>
<th>355</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sizewell</td>
<td>0.09</td>
<td>0.01</td>
<td>0.017</td>
<td>0.12</td>
<td>14</td>
</tr>
<tr>
<td>Surry 1</td>
<td>0.094</td>
<td>0.094</td>
<td>0.40</td>
<td>0.59</td>
<td>0.76</td>
</tr>
<tr>
<td></td>
<td>0.26</td>
<td>0.14</td>
<td>0.008</td>
<td>0.41</td>
<td>0.03</td>
</tr>
<tr>
<td>Ocone 3</td>
<td>0.009</td>
<td>0.15</td>
<td>0.57</td>
<td>0.74</td>
<td>6.8</td>
</tr>
<tr>
<td></td>
<td>0.025</td>
<td>0.23</td>
<td>0.012</td>
<td>0.26</td>
<td>0.27</td>
</tr>
<tr>
<td>Biblis B</td>
<td>0.013</td>
<td>0.38</td>
<td>-</td>
<td>0.39</td>
<td>0.67</td>
</tr>
<tr>
<td></td>
<td>0.036</td>
<td>0.57</td>
<td>-</td>
<td>0.61</td>
<td>0.02</td>
</tr>
<tr>
<td>Ringhals 2</td>
<td>0.12</td>
<td>0.024</td>
<td>0.46</td>
<td>0.61</td>
<td>24.5</td>
</tr>
<tr>
<td></td>
<td>0.34</td>
<td>0.04</td>
<td>0.01</td>
<td>0.39</td>
<td>0.98</td>
</tr>
</tbody>
</table>

Note
The Sizewell 'First Estimates' were evaluated on a basis comparable with that used in WASH-1400, and are conservative. The 'Second Estimates' represent a probabilistic reduction, anticipating some of the reduced source term research then in progress. Even the second estimates overestimate the delayed releases in the Biblis B and Ocone 3 studies.
Examples of these requirements are those related to the reactor protection system, the decay heat removal function, the auxiliary feedwater system, and the AC emergency power system. With the current available operating experience and accumulated insights about NPP safety, regulators regard plant safety as a function of plant design, construction, plant operations and operations-design interactions. A complete reliance on systems performance requirements, in a case-by-case fashion may or may not lead to safety levels lower than those intended by the standard setter, unless regulatory evaluations are expanded to consider interactions and potential adverse impacts on an overall plant safety performance level.

As the methods of Probabilistic Risk Assessment (PRA) approach maturity, regulators recognized its strengths and potential. PRA integrates into a uniform methodology, the relevant information about plant design, operating practices, operating history, hardware reliability, human reliability, the physical progression of accidents, and potential environmental and health effects in case of radioactive releases, in a systematic manner. It uses both logic models and physical models. The logic models define the combinations of events (sequences) that could result in a core damage accident and are used to determine the frequencies associated with each combination. The physical models depict the progression of the resultant accident and the severity of damage to the plant. For example, the combinations of events that can lead to a LOCA, and the probabilities that these combinations will occur, are
identified by a logic model, while, amongst others, the analysis of
the containment response to the accident is based on a physical model.

Public health effects and economic losses resulting from a core damage
accident, which may also involve the release of radionuclides into the
environment, can be assessed by means of environmental transport,
protective action response, and consequence models. The environmental
transport models use site-specific data to predict the spread and fallout
of the released radionuclides. The consequence models use demographic
data to predict the health effects expected to occur in the surrounding
population.

The results of the risk assessment are analyzed and interpreted to
identify the plant features and operational practices that are the most
significant contributors to the frequency of core melt, to vulnerability
of the containment, and to the frequency and amount of radioactive
releases and to risk. They can also be used to generate a variety of
qualitative information regarding the events and failures associated with
various consequences.

PRA is subject to a number of known weaknesses and limitations. Maturity
level, weaknesses, and limitations in each segment of a full-scale PRA are
discussed in detail in References 1, 2. Among these limitations are gaps
and inadequacies in the data base, modeling of core damage phenomenology,
external events, failure dependencies, human performance and equipment
behavior under accident conditions. Performance of realistic analyses is
always one of the goals claimed in PRA studies. However, when
information is lacking or controversy exists the analyst has no choice
but to introduce conservatism, increase uncertainties or exercise his
judgment.

The problems mentioned above as a consequence that each risk analysis in
the end provides an estimate of risk and automatically involved subjec-
tivity. Likewise the deterministic safety evaluation cannot be performed
without interjection of subjectivity. It is less apparent in this case,
however, than in the case of probabilistic methods. In both cases, the
engineering experience provides a substantial basis for evaluation.

Irrespective of whether deterministic or, as in risk analyses,
probabilistic methods are applied, the experience and ability of the
expert are crucial for the quality of a technical analysis.

It is important to note that the recognition of negative aspects of the
PRA, contained in the preceding discussion does not mean that valuable
insights still cannot be derived from existing PRA results. Insights are
based on information extracted from the analysis of quantitative results
including point estimates, uncertainties, results of sensitivity evalua-
tions, and possibly results of importance analysis. The quality of
derived insights reflects the quality of this information base. An
insight based on information that exhibits reasonable uncertainties and
robustness to modeling assumptions should be given a heavier weight in
decision making compared with other insights lacking these qualities. Understanding all of the significant strengths and limitations on part of the decision maker will enable him to make a more effective use of all available analyses including the information obtained from deterministic and probabilistic evaluations. There are many types of regulatory decisions, and the weight given to the quantitative PRA results should vary depending on the degree of precision necessary and attainable.

2.0 PRA Regulatory Applications (1,2)

It is now recognized that a PRA, due to its realistic integrated approach, presents the best available information concerning the specific ways in which critical safety functions at nuclear power plants can fail to be performed. This is valid in spite of PRA known limitations and even though PRA models may be incomplete and evaluation uncertainties may be large. The wide spectrum of activities at NRC and the nuclear industry can utilize the PRA information to guide and better focus these activities, as appropriate, in order to improve the safety performance of individual nuclear power plants. Since the resources available for regulatory activities are always limited, PRA insights provide an additional tool to permit decision makers to allocate these resources to areas most likely to reduce risk, or to narrow and limit existing uncertainties.

The use of PRA evaluations at NRC is marked by a steady increase and wider acceptability. The scope and level of technical detail in these evaluations is controlled by the objectives of the intended applications. Among these applications are, allocation of resources, setting of regulatory priorities, resolution of safety issues, identification of outlier plant features, development of a better understanding of the nature of severe accidents and their consequences, and assurance of safety margins within existing designs. Some of these applications are briefly covered below in order to illustrate the extent of PRA regulatory usage.

2.1 Technical Specifications

Nuclear power plants must operate in compliance with technical specifications which are operational limitations or requirements specified to assure an acceptable level of safe performance. Technical Specifications include Limiting Conditions for Operations (LCOs), surveillance testing requirements, safety systems setpoint limits, and administrative controls. Regulators are currently involved in an effort to determine how PRA information could be used to establish the need and the character of technical specifications. It is expected that these requirements shown to be too restrictive and with no significant risk impact will be relaxed.

As an example, the removal of a piece of equipment or train of equipment during maintenance, repair, and testing activities, reduces the level of built-in redundancy and increases the unavailability of involved safety systems. Outage time for these activities represent a period of increased vulnerability to accidents, until the equipment or trains are
7

Constraints on Allowed Outage Times (AOTs) are imposed as part of the operating licenses. These constraints are referred to as LCOs. Exemptions from LCOs and extensions of outage times beyond those allowed by technical specifications are frequently requested by licensees. Sensitivity evaluations of PRA models are used to assess their impact on system unavailability, safety function unavailability, or a risk indicator like core damage frequency. Results of the analysis are sometimes used to assist in making decisions. Other examples include revisions in Reactor Protection Systems testing requirements and extensions in Diesel Generator LCOs.

2 Applications in Inspection and Enforcement Programs

Information from PRAs can also be used to guide the overall allocation of resources in inspection and enforcement programs. A catalog of information derived from PRAs indicates that certain surveillance tests and maintenance activities are significant contributors to the estimated frequency of plant damage or to risk. If a class generic risk profile is available, it could be used to determine importance measures regarding critical surveillance testing and maintenance activities that can, if not done properly, significantly alter the predicted core melt frequency or risk. These important measures could be used in assigning priorities for inspection auditing, the training of operators and maintenance personnel, and reliability assurance program requirements. The generation of such information for each class of operating plants provides a rough ordering of important operating activities that should assist a reactor inspector

8

In efficiently directing the inspection effort at a given facility. Similarly, generic insights (available by reactor class) assist both the licensee and the regulator in identifying and preventing potentially significant operational occurrences at a plant, even if a plant-specific PRA is not available.

2.3 Rulemaking and Regulatory Guidance

The insights derived from PRAs also provide additional information to aid in rule-making and the development of regulatory guidance. Such activities would be aimed at reducing risk or relaxing regulatory requirements that do not have a significant impact on risk and identifying those worthy of additional refined examination.

The research arm of NRC has initiated a program to review current light water reactor regulatory requirements to see if some could be relaxed or eliminated to reduce regulatory burdens without compromising public health and safety. Analyses are being performed to assess the effects of streamlining regulatory requirements in some selected regulatory areas. Probabilistic risk assessment, play a central role in evaluating the risk and safety significance of streamlining regulatory requirements. Analyses covers a range of different types of regulatory requirements, and a range of different degrees of regulatory relaxation. Identification of a set of regulatory requirements among existing regulations for this review process is sensitive to public responses to the published Federal Register notice, and to feedback from the nuclear industry and NRC staff.
2.4 The Severe Accident Program (4, 5, 6)

The U.S. Nuclear Regulatory Commission has recently issued a policy statement on severe accidents which provides criteria and procedural requirements for the licensing of new plants, and sets goals and a schedule for the systematic examination of existing plants. The implementation program for this policy statement incorporates three major elements. The first element is to formulate an integrated, systematic approach to an examination of each nuclear power plant now operating or under construction for possible significant risk contributors that might be plant specific and might be missed in the absence of systematic search. The second major element is to develop guidance on the roles of PRA studies in the approval of new applications. The last and third major element is the modification of the regulatory rules, guides and other regulatory practices not only to reflect those changes in our scientific understanding arising from our present and continuing research effort in severe accident releases ('source term'), but also to reflect additional insights arising from severe accident research, such as the need for new performance criteria on containment behavior which will be done in conjunction with efforts to establish safety goals for Nuclear Power Plants.

The systematic approach associated with these elements includes the development of guidelines and procedural criteria for the examination of NPPs and identification of potential vulnerabilities to severe accidents. These guidelines will count heavily on existing PRA experience with a special emphasis on perspectives gained in the SARP and IDCOR programs. Development is driven by a realization in the nuclear community in general, and at NRC in particular that PRA experience combined with an effective and carefully engineered guidance can be used to capture the majority of conclusions that a full scope PRA can yield at a reduced cost, and then to provide further motivation for a more detailed search for outliers that may be unique to a specific NPP. We realize that this process is neither simple nor straightforward, and that an effective methodological approach has to be engineered with extreme caution and should have built in flexibility to change with future experiences. This guidance will be developed in the near future. Before it assumes its final form, it will be tested in case studies and it will be exposed to critique from the nuclear community in general and PRA practitioners in particular.

3. Summary and Overview

As the methods of probabilistic risk assessment approach maturity, regulators recognize its strengths and potentials. Among the strong points of PRA are its integrated and systematic approach to NPP safety, its consideration of failure dependencies, interaction among systems and their support systems, its detailed consideration of the human element, and its ability to make an explicit statement about the magnitude of uncertainties associated with evaluation results. PRA insights and methods are finding increasing acceptability among regulators. This development is clear from the PRA applications addressed above.
However, this acceptability is still marked with caution, since decision makers are also aware of limitations and weaknesses of PRA techniques, that prevent PRA usage as the sole basis of regulatory decisions. At the same time, regulators are also aware of the strengths and weaknesses of the conventional deterministic approach to regulation. The current practice at NRC is to use both types of evaluations and operating experience as an input to decision making. This practice when modeled in a systematic integrated framework will assure a consistent base for making decisions, and carries the promise of an even greater use of PRA methods in the immediate future.

Development of such an integrated approach is currently under consideration and it may envelope regulatory activities related to nuclear power plant operations. In this integrated approach accumulated experiences from PRA studies will be relied upon to define scopes and level of technical details for safety evaluations. Issues of regulatory concern will not be investigated in isolation of each other unless there is sufficient technical basis to assure that resolution of an issue would not adversely influence others. Similarly, proposed operational and design modifications are not to be evaluated from a single system or subsystem performance viewpoint, but rather from an overall plant safety performance viewpoint. Cost-benefit evaluations will play a central role in ranking sets of proposed alternative design and operational modifications.

Most of the discussed PRA applications have been introduced in the regulatory activities in the past few years. It is evident that PRA models are being used at NRC and will be reused, refined, and updated as appropriate. It is also recognized that the nuclear industry in general has steadily increased its use of PRA. There is considerable motivation for individual licensees to develop and use their own PRA models and to establish their own safety assurance programs to maintain and improve on the achieved level of plant safety performance.

References


5. Z. R. Rosztoczy and T. P. Speis, "Regulatory Considerations of Severe Accidents", Proceedings of the International ANS/EHS Topical Meeting on Thermal Reactor Safety".

A PRA BASED INTERACTIVE SYSTEM
FOR PLANNING
REACTOR INSPECTION ACTIVITIES

Dr. James C. Glynn
Division of Risk Analysis and Operations
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

A. INTRODUCTION

In 1975, the publication of the U.S. Reactor Safety Study (WASH-1400) provided the nuclear industry with a mechanism to logically assess a plant risk (core melt frequency and off-site consequences) by combining information on faults associated with those systems, components and human actions that are required for safe operation. Eager to capitalize on the inherent usefulness of the PRA’s logic structures, e.g., fault and event trees, and its quantitative results, e.g., system failure probabilities, several U.S. studies were then initiated to see how this risk information could be integrated into the NRC's Regulatory process, in particular its inspection and enforcement (IE) program. The results of these initial studies however, met with little success in developing a methodology that would provide an inspector with the PRA data that could make his decisionmaking less subjective. As time went on however, and the number of U.S. operating plants of multiple designs began to increase significantly, the NRC’s Division of Research (RES) chose to re-visit this matter by funding its own project, which again was to see if and how PRA data could be melded into the inspection process. This renewed interest by RES in investigating PRA application for inspection purposes was further enhanced at that time by the large number of plant specific PRA being published by industry and the NRC e.g., IREP program, whose risk insights seemed to many to offer considerable promise in such areas as plant reliability and safety.

Accordingly, in 1983 RES initiated a program entitled, "Risk Assessment Application to NRC Inspection" whose initial focus was to thoroughly study the IE inspection program e.g., responsibilities and actions of resident inspectors, and then try to establish the relationships between plant risk and inspection decisions, before focusing on the process of identifying, accumulating, and formatting large volumes of PRA information into a system for use by an inspector. This particular approach to the project, that is--requiring the PRA analyst to first understand and witness those risk relevant situations and decisions that are a daily part of an inspectors job, is now seen to perhaps have been the most important programmatic decision leading to the successful development of a PRA based inspection system. For example, it was found that the information to support an inspection decision needed to be: (1) readily accessible, (2) free of PRA jargon, (3) readily recognizable to inspectors with varied technical backgrounds as to its usefulness, and (4) responsive to the types of decisions inherent in an inspector’s IE program e.g., mandatory inspection procedures.

This research study has now proceeded to where a very promising methodology has been developed, using the Arkansas Nuclear Power Plant PRA as its test case, that can supply reactor inspectors with a significantly usable data base for inspection decisionmaking activities through the use of a desk top PC-computer. The methodology specifically provides information to the inspector for daily inspection planning based on the risk relevance of the immediate plant status, or, for longer range inspection planning, information that would address his responsibilities for completing specifically required inspection tasks. The methodology is now being incorporated into a system called PRISIM (Plant Risk Status Information Management) that will contain an inspection oriented data base in conjunction with an interactive capability to enable decisionmakers such as e.g., inspectors, reliability engineers etc. to gain access to essential information, put it into meaningful form, and use it to improve their productivity.

B. PRISIM SYSTEM DESCRIPTION:

The Plant Risk Status Information Management System (PRISIM) is a decision-oriented, user-friendly, menu-driven program that contains data base management and interactive routines to aid inspectors in allocating their efforts towards those areas of greatest impact on plant safety. The program was written for an IBM XT personal computer with special high resolution graphics and a 20 mega-byte hard disc. PRISIM’s controlling feature is a data base manager that essentially performs two main functions for the user: (1) it selects screen images from the PRISIM data base and displays them on a monitor, and (2) controls the PRISIM interactive routine—the portion of the program that calculates the risk status of the plant at a particular time—and then displays the results of these calculations on the monitor. The PRISIM data base contains pre-processed or "canned" information that is relevant regardless of the plant's status, whereas the interactive routine provides the user with PRA data that has been updated to reflect the status of the plant at the moment. The following are brief summary descriptions of the types of information presented on PRISIM data base screens and the types of information obtained from PRISIM’s plant status interactive routine.

B.1 PRISIM DATA BASE

The information contained in PRISIM’s data base consists of:

Dominant Accident Sequences

The accident sequences that make the largest contributions to a plant's risk are listed in PRISIM. An inspector can command PRISIM to display information on a particular accident sequence. He will then see a description of the accident sequence, a listing of the most important causes of the sequence, and a description of the relevant recovery actions.

Safety-Related System Importances

The PRISIM data base provides four types of risk importance measures for safety-related systems: (1) safety assurance importance, (2) risk reduction importance, (3) risk sensitivity importance, and (4) risk significance importance. Table 1 contains a qualitative definition of these four importance measures from which specific inspection activities can be correlated unambiguously.

Safety-Related Subsystems

PRISIM provides the same four types of risk importance measures for safety-related subsystems that it provides for systems. It also lists the surveillance tests for each subsystem and indicates whether each test is an integral test. If a test is not integral, the components that are not tested are identified.

Safety-Related Components

In addition to the same four importance measures, PRISIM provides modified information if a particular component is of service. This information includes lists of single component failures which would disable the system if a specified component is taken out of service. These failure modes are of two categories: those that are covered by the license in response to the plant's technical specifications and those that are not.

Support System Interfaces

To identify dependencies among front-line safety systems and support systems (e.g., electrical power and service water), PRISIM provides, for each system, a table that shows the support services required by components in that system.

Component Failure Data

Two types of information on component failure data are incorporated in the PRISIM data base. First, PRISIM includes summaries of licensee event reports (LERs) by component type for the plant. Second, there are comparisons of plant-specific failure data with industry-averaged failure data for plant equipment. These comparisons highlight plant equipment that is more or less reliable than the industry average for equipment of the same type.

Fire Zones

PRISIM provides a ranking of fire zones at the plant with respect to their importance to risk. An assumption that is inherent in these rankings is that a fire will fall all equipment in the zone where it occurs.

B.2 PRISIM INTERACTIVE ROUTINE

The interactive routine allows the inspector to manually input a plant status into the program, i.e., components that are currently out of service, and receive instantaneously the recomputed core melt frequency and the dominant failure scenarios for the new plant configuration. Specifically, the interactive routine has the capability to generate the following information for a given plant state:

- The factor by which the instantaneous core melt frequency increases when the specified set of components is out of service.
- The most important failure scenarios for core melt ranked according to their expected frequencies of occurrence.
- A ranking of the unfailed equipment according to their relative contributions to the instantaneous core melt frequency (risk reduction).
- A ranking of the failed equipment according to the benefit of restoring each to service (risk response).
- A ranking of the unfailed equipment according to their relative contribution to instantaneous core melt frequency if the equipment were to be taken out of service (safety assurance).

The factor by which core melt frequency increases due to components being out-of-service is not intended to be literally interpreted, but rather to serve as an index on which an inspector can assess the risk implications of a plant state and then decide whether he should focus his immediate attention on seeing to it that he makes those decisions that might prevent any further increase in plant risk. The interactive routine for the AND-1 plant contains only the dominant minimal cutsets which are sufficient to allow the program to retain the failure modes that represent about 85 percent of the total expected core melt frequency for the AND-1 plant. The extraordinary value of the interactive
routine can be found in its capability to provide an inspector with: (1) a strong case as to whether he should focus his attention on the risk associated with a particular plant status, (2) a ranking of the important plant equipment that can be correlated to a specific inspection action, and (3) assurance that the complex interaction effects arising from potential failures of support systems that can disable safety systems, hereafter generally beyond the capability of an inspector, have been properly accounted for in his decision-making process.

C. APPLICATION OF PRISIM TO INSPECTION

The PRISIM program contains an architecture that was developed to facilitate the decision-making process that an inspector constantly finds himself involved in. Simply put, in the course of performing his daily activities, an inspector must first make the decision, perhaps unwittingly, to either focus his attention in response to existing plant conditions or to inspect specific plant design/operating features in accordance with the requirements of the procedures contained in the U.S. NRC's Inspection program (IE Manual). The following are brief descriptions as to how PRISIM responds to whichever decision type that an inspector chooses to follow and a demonstration of exactly what information is provided the inspector to assist him in implementing this decision.

C.1 SCHEDULING DECISIONS

At the present time, the PRISIM program contains inspection information for 15 of the most frequently used inspection procedures as defined in the IE Manual. These procedures describe various types of inspections to be performed and they allow a great deal of latitude in terms of where the inspector should focus his attention. Accordingly, when an inspector is faced with the decision as to how to schedule which components should be inspected most often, PRISIM will assist him by providing the results of systematic analyses of each procedure identifying: (i) the specific inspection decisions associated with the procedure, (ii) the relevant procedural decision categories, i.e., witness corrective maintenance, that can then be directly correlated to the various importance measures and present this information in a form that would be readily useful to him. Other types of information provided in PRISIM that are relevant to inspection scheduling decisions are trends in component failures and how component reliability performance at the plant compares to other plants. All of these types of information discussed above can be used by an inspector to judge (schedule) which components should be inspected most often. Figures 3-8 provide exact replicas of the information PRISIM can provide an inspector. For example, if he were to choose to implement Procedures 71707, we can see from Figures 3-8 those decisions facing the inspector e.g., which safety-related systems should be emphasized, and the relevant PRA information available for him to schedule what systems he should most frequently focus his attention on. PRISIM's detailed matrix of information for scheduling decisions is based on a methodology that will be described in a soon to be released NUREG/CR report. This methodology can be further used as a means to assess the overall efficacy of an inspection program's procedures from a risk perspective.

C.2 PLANT RESPONSE DECISIONS

The PRISIM system further provides an inspector with an extremely useful tool to assist him in judging whether the risk associated with a current plant status warrants his immediate attention. This can be accomplished simply and rapidly after he has determined the actual plant operational status e.g., components known to be out of service. The inspector would then call on PRISIM's interactive routine, input this specific plant information and almost instantaneously be informed of the effect these conditions have on the plant's overall core melt frequency e.g., change in plant risk index. Assuming the risk index registers a significance increase, the inspector can either continue to use the interactive routine in deciding where to focus his efforts or else he can directly obtain information from PRISIM's data base management portion to assist him in deciding where he should direct his attention. The specific information available to him through both the interactive and the data base management portions has been discussed previously in this paper; however, the following example illustrates very clearly how the interactive system would provide an inspector important information to: (1) decide if he should focus his immediate attention on the plant status, and (2) decide where his attention should be focused based on prioritization rankings of the importance of each piece of equipment in terms of it either being returned to service or removed from service.

EXAMPLE: Assume the inspector has visited the control room and found that a valve in the Emergency Feedwater System (EFW) and a valve in the Battery and Switchgear Emergency Cooling System (ECS) are out of service. He consults PRISIM to determine the significance of this plant status.

The inspector is first presented with the option of obtaining safety-related information through a direct access path or an inspection procedure path. If he selects the direct access path, as in this example, the user is first presented with a list of information categories addressed in PRISIM (Figure 9). For this case, he selects "risk implications of the current plant status." He is then presented with two options that allow him to specify the out-of-service components (Figure 10). If the inspector selects the "schematics" option, as Figure 10 indicates he does, he will be presented with a list of safety-related systems (Figure 11). Having selected the schematic for the EFW, the inspector will next see the screen appearing in Figure 12. As indicated by the cursor's position on the schematic, the inspector specifies the appropriate valve in the EFW that is out of service. The inspector then returns to the system menu and selects the ECS to specify the valve in this system that is now to be out of service (Figure 13 and 14).
After the inspector has specified the out-of-service components for
the EFW and ECS, he selects the "END OF INPUT" option and is presented
with a screen (Figure 15) that show three things: (1) the factor of
increase in core melt frequency, (2) the components specified as
being out-of-service, and (3) the inspector's options for additional
information. As indicated in the figure, the core melt index is
increased by a factor of 70 when the two valves are out-of-service.

To obtain information that will help him decide how to focus his
efforts on the components not known to be out of service, the user
selects the "ranking of safety-related equipment" option at the
bottom of the screen. He is then presented with a screen that pro-
vides a ranking of equipment (Figure 16). For this example, the EFW
Train A-to-Train B crossover line is one of the listed components and
the inspector knows that maintenance is to be performed on a valve in
the line. To assess the impact of performing this maintenance, the
user specifies the crossover line as an additional out-of-service
condition (Figure 17). He is then presented with an updated increase
in core melt frequency (Figure 18), which he can now use as an aid in
deciding whether to respond to the plant status.

The above example was chosen to demonstrate the ease by which the
PRISIM interactive routine can inform an inspector that his immediate
attention should be to see that plant conditions that could further
exacerbate the risk are determined and possibly therefore avoided.
In this regard, it is worth noting that the equipment ranking,
Figure 16 is a direct consequence of the plant status and could only
be obtained from PRISIM's interactive system and not the PRA itself.
The data base management system could be used also by the inspector
as an aid in assisting him to effectively focus on the risk of the
plant status.

Conclusions
The initial development of the PRISIM system for use at the Arkansas Nuclear
Unit-1 plant by the NRC's resident inspector will be completed in July 1986. A
period of testing and evaluating the system will be performed over a three
month period so that information can be obtained in terms of how, when and
where this system can be most helpful in inspection planning. During this same
period, work will begin on the development of similar systems for the Peach
Bottom, Surry, Sequoia, Grand Gulf, and Zion nuclear plants. This multi-plant
effort will produce inspection systems identical to the ANG-1 system; however,
several of the NRC's research programs will be integrated into the process in
an effort to produce a methodology for rapidly translating PRA results into
useable regulatory tools.

In parallel with the development of the decisionmaking systems for inspectors,
a PC based prototype system will be available this summer with the capability
to estimate changes in plant risk as a function of component failure rates,
human error probabilities, allowed outage times and surveillance test
intervals. This initial system will use ANG-plant as its model and be made
available to NRC's regulatory engineers for their evaluation and use. Other
potential areas where risk based decisionmaking systems will be investigated
are training and plant risk evaluations.

Reference:
(1) Risk Assessment Application to NRC Inspection, Technical
(2) Risk Assessment Application to NRC Inspection, Interim
### Table 1: Definitions of Measures of Importance

<table>
<thead>
<tr>
<th>Measure of Importance</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety Assurance</td>
<td>The factor by which risk increases when the equipment is out of service.</td>
</tr>
<tr>
<td>Risk Response</td>
<td>The factor by which risk decreases when the out-of-service equipment is returned to service.</td>
</tr>
<tr>
<td>Risk Reduction</td>
<td>The decrease in risk when the equipment is assumed to be perfectly reliable. (When normalized to the average risk, these results represent the likelihood that the equipment would contribute to a core melt if a core melt were to occur.)</td>
</tr>
<tr>
<td>Risk Sensitivity</td>
<td>The rate at which the risk changes with changes in the equipment failure probability (or frequency).</td>
</tr>
<tr>
<td>Risk Significance</td>
<td>Combined risk reduction importance and risk sensitivity importance. (Equipment is grouped according to risk reduction importance. Equipment with a high risk sensitivity importance is then moved to the next higher group.)</td>
</tr>
</tbody>
</table>
INSPECTION PROCEDURES ADDRESSED IN THIS PROGRAM

<table>
<thead>
<tr>
<th>PROCEDURE NUMBER</th>
<th>INSPECTION PROCEDURE TITLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>71707</td>
<td>Operational Safety Verification</td>
</tr>
<tr>
<td>61793</td>
<td>Monthly Surveillance Observation</td>
</tr>
<tr>
<td>62703</td>
<td>Monthly Maintenance Observation</td>
</tr>
<tr>
<td>71711</td>
<td>ESF System Malfunction</td>
</tr>
<tr>
<td>92700</td>
<td>Onsite Followup of Events at Operating Reactors</td>
</tr>
<tr>
<td>92702</td>
<td>Onsite Followup of Written Reports of Nonroutine Events</td>
</tr>
<tr>
<td>92703</td>
<td>IE Bulletin/Immediate Action Letter Followup</td>
</tr>
<tr>
<td>92704</td>
<td>Review of Plant Operations</td>
</tr>
<tr>
<td>92705</td>
<td>Followup IE Circulars, Information Type Bulletin</td>
</tr>
<tr>
<td>92706</td>
<td>Surveillance - Refueling</td>
</tr>
<tr>
<td>92707</td>
<td>Maintenance - Refueling</td>
</tr>
<tr>
<td>92708</td>
<td>Independent Inspection Effort</td>
</tr>
<tr>
<td>92709</td>
<td>Followup - Headquarters Requests</td>
</tr>
<tr>
<td>92710</td>
<td>Followup - Regional Requests</td>
</tr>
</tbody>
</table>

Figure 2

DECISIONS ASSOCIATED WITH INSPECTION PROCEDURE 71707—OPERATIONAL SAFETY VERIFICATION—FOR WHICH PRA INFORMATION IS AVAILABLE

DAILY INSPECTION

1. What emphasis should be given to the existing plant status? (Interactive Routine)

WEEKLY INSPECTION

1. Which safety-related subsystems should be emphasized?

BIWEEKLY INSPECTION

1. What safety-related tag-outs should be emphasized?

2. When a plant tour is performed, which fire zones should be emphasized?

3. Based upon the information collected during the plant tour, what emphasis should be given to the existing plant status? (Interactive Routine)

Figure 3
SUBSYSTEMS GROUPED BY RISK SIGNIFICANCE IMPORTANCE

HIGH RISK SIGNIFICANCE

Battery and Switchgear Emergency Cooling System--Chill Water Train A
Battery and Switchgear Emergency Cooling System--Chill Water Train B
Emergency Even DC Power
Emergency Feedwater Initiation and Control System--Initiation Channel A
Emergency Feedwater Initiation and Control System--Vector C
Emergency Feedwater System--Train B (Turbine Driven)
Emergency Odd AC Power
Emergency Odd DC Power

→ (CONTINUED)

Figure 4

SUBSYSTEMS GROUPED BY RISK SIGNIFICANCE IMPORTANCE (CONTINUED)

HIGH RISK SIGNIFICANCE

Emergency Onsite AC Power
Emergency Onsite DC Power
High Pressure Injection System--Train C
Service Water System--Loop 1
Service Water System--Loop 2
Safety/Relief Valves (failure to close)

MODERATE RISK SIGNIFICANCE

Emergency Even AC Power
Emergency Feedwater Initiation and Control System--Initiation Channel B

→ (CONTINUED)

Figure 5
MODERATE RISK SIGNIFICANCE

Emergency Feedwater System—Train A (Motor Driven)
Engineered Safeguards Actuation System—Analog Channel 1
Engineered Safeguards Actuation System—Analog Channel 2
Engineered Safeguards Actuation System—Analog Channel 3
High Pressure Injection System—Trains A and B
Low Pressure Recirculation System—Train A
Low Pressure Recirculation System—Train B
Safety/Relief Valves (failure to open)

(CONTINUED)

LOW RISK SIGNIFICANCE

Battery and Switchgear Emergency Cooling System—Refrigerated Unit A
Battery and Switchgear Emergency Cooling System—Refrigerated Unit B
Core Flood System—Train A
Core Flood System—Train B
Emergency Feedwater Initiation and Control System—Vector D
Engineered Safeguards Actuation System—Digital Channel 1
Engineered Safeguards Actuation System—Digital Channel 2
High Pressure Recirculation System—Trains A and B
High Pressure Recirculation System—Train C

(CONTINUED)
SUBSYSTEMS GROUPED BY RISK SIGNIFICANCE IMPORTANCE (CONTINUED)

LOW RISK SIGNIFICANCE

Low Pressure Injection System--Train A
Low Pressure Injection System--Train B
Reactor Protection System--Channel A
Reactor Protection System--Channel B
Reactor Protection System--Channel C
Reactor Protection System--Channel D

Figure 8

CATEGORIES OF SAFETY-RELATED INFORMATION

1. Risk implications of the current plant status
2. Dominant accident sequences
3. Safety-related systems
4. Safety-related subsystems
5. Safety-related components
6. Support system interfaces
7. Component failure data
8. System testing/surveillance

Figure 9
OPTIONS FOR SPECIFYING OUT-OF-SERVICE COMPONENTS

1. Schematics
2. Component list

SAFETY-RELATED SYSTEMS FOR WHICH SCHEMATICS ARE AVAILABLE

1. North Battery and Switchgear Rooms Emergency Cooling System
2. South Battery and Switchgear Rooms Emergency Cooling System
3. DC Power System
4. Emergency AC Power System
5. Emergency Feedwater Initiation and Control System
6. Emergency Feedwater System
7. Engineered Safeguards Actuation System
8. High Pressure Injection System
9. High Pressure Recirculation System
10. High Pressure Pump Cooling System
(CONTINUED)
SAFETY-RELATED SYSTEMS FOR WHICH SCHEMATICS ARE AVAILABLE

1. North Battery and Switchgear Rooms Emergency Cooling System
2. South Battery and Switchgear Rooms Emergency Cooling System
3. DC Power System
4. Emergency AC Power System
5. Emergency Feedwater Initiation and Control System
6. Emergency Feedwater System
7. Engineered Safeguards Actuation System
8. High Pressure Injection System
9. High Pressure Recirculation System
10. High Pressure Pump Cooling System

(CONTINUED)
RISK IMPLICATIONS OF THE CURRENT PLANT STATUS

70 IS THE RISK FACTOR WITH THE FOLLOWING EQUIPMENT OUT OF SERVICE

Emergency Feedwater System—Train A fails
Battery and Switchgear Room Cooling System—CN Train A fails

MENU FOR ADDITIONAL INFORMATION

1. Ranking of safety-related equipment
2. Ranking of core melt scenarios
3. Improvement from repair
4. Return to Master Menu
1. Battery and Switchgear Room Cooling System--CW Train B fails
2. Blockage of EFW Train A-to-Train B Crossover Line
3. Both safety/relief valves fail to reclose
4. Auxiliary Cooling Water System Isolation Valve CV3643 fails
5. Intermediate Cooling Water System Isolation Valve CV3820 fails
6. EFW Initiation and Control--Vector Signal Path 1D-32D fails
7. EFW Initiation and Control--Vector Signal Paths 2D-22D and 3D-22D fail
8. Both safety/relief valves open and fail to reclose
9. High Pressure Injection System Pump P36C fails
10. EFW Initiation Signal Paths AC61-AC64 and BD61-BD64 fail

Esc to return to the Selection Menu

Figure 16

EMERGENCY FEEDWATER SYSTEM SCHEMATIC

MINIMUM FLOW RECIRCULATION TO CST TO DISCHARGE LINE

SG E24A

FW13A TRAIN B

P7B

CY2827

C-2

CVX-4

TURBINE

CONDENSATE STORAGE TANK

MINIMUM FLOW RECIRCULATION TO CST TO DISCHARGE LINE

SG E24B

FW13B TRAIN A

P7A

TURBINE

SYSTEM MENU END OF INPUT

Figure 17
USE OF THE LIMERICK PRA IN SAFETY ASSURANCE

A. Richard Dielerich, P.E.
Philadelphia Electric Company
2301 Market Street
Philadelphia, PA 19101
215-841-4316

Philadelphia Electric Company (PECo) has had a long involvement in Probabilistic Risk Assessment (PRA) dating from the use of its Peach Bottom Atomic Power Station (2-1050 MWe, BWR, Mark I Units) as a reference plant for WASH 1400. Applications within the Company are not limited to nuclear power plants, but also include studies related to electric power transmission and fossil power plants. Understanding of the potential for PRA analyses and insights has led to PECo's current program to use the PRA in support of operations and engineering for Limerick Generating Station, Unit 1 (1050 MWe, BWR, Mark II).

1. BACKGROUND
The Limerick PRA was done in response to an NRC request in 1980 to address concerns regarding the relatively higher population density surrounding the Limerick site. The initial internal events analysis was later supplemented by the Severe Accident Risk Analysis (SARA) which included external events, an expanded uncertainty analysis and an offsite consequence analysis for all sequences. The accident progression in containment was modeled using WASH 1400-era computer codes. Time constraints precluded widespread PECo involvement in the early efforts, but later in the process the fault and event trees underwent a detailed review by PECo Personnel. The result was a state-of-the-art level 3 PRA which accurately represented the Limerick plant as designed in 1981.

In risk terms, the Limerick PRA indicated the plant posed no undue risk to the public, with overall consequences similar to the WASH 1400 reference plant. Core Damage Frequency point estimates are presented in Figure 1 (end of text).

The Limerick PRA process was accompanied by significant review efforts by both the ACRS and the NRC Staff, assisted by Brookhaven National Laboratory and others. These groups expressed interest in PECo's continuing the use of the PRA after the plant was in service. Early in our ACRS discussions we stated our intent to keep the PRA "up-to-date" with respect to the plant configuration. As the process of ACRS hearings was nearing an end in the fall of 1984, we expanded on our previous presentations, describing the outline of plans which are described in this paper.

The NRC Staff also vigorously endorsed the continuing use of the Limerick PRA. Nine "Key Elements of Continued Use of Risk Assessments", also recommended for implementation at Indian Point, were proposed by the Staff in correspondence. In its document summarizing the review of the Limerick PRA (NUREG-1068, "Review Insights on the Probabilistic Risk Assessment for the Limerick Generating Station") the Staff reiterated its recommendation that PRA use be continued in a safety assurance program which would serve to:

1. Reflect PRA insights into procedures and operating staff training.
2. Revise procedures where such changes would reduce risk.
3. Analyze or identify modifications which may reduce risk.
4. Integrate risk-based thought and analyses into its organization.
5. Revise failure, operator error and initiator data based on actual plant experience.

Any one of these items is worthy of a lengthy discussion. The intent of each recommendation is included in the PECO plans or the framework is established to pursue it.

II. PECO PROGRAM

II.A Initial Evaluation
A study was initiated to examine the options available for a program which would effectively implement PECO's intent to continue to use the Limerick PRA. The goal of the study was to identify the technical bases of continued PRA use (e.g., risk measure, types of initiators, level of detail, systems included, etc.), an effective organizational approach, a prioritization of technical applications and a flexible implementation plan. The consultant for this effort examined a wide range of options, discussed them with a number of PECO personnel and recommended a program which was in large part adopted. The major areas are discussed below.

II.B Technical Bases
Risk measure: Core Damage Frequency - This was selected as an appropriate, widely used comparative measure which adequately acts as a surrogate for risk to the population in general as well as being a close representation of financial risk to the owner. Examination of the use of offsite consequences as the primary measure indicated that significant resources would be required to generate results. The higher uncertainty in this area dictated that the risk measure be adopted at a level more directly affected by plant design and operations.

Evaluation of fission product release from the plant has the advantage of achieving consideration of fission product cleanup mechanisms and containment functions. However, changes in the accepted understanding of fission product transport and in-containment phenomena would be time consuming to incorporate and would have greater effects on results than changes in the plant model.

PECO has the capability to analyze these factors using the MAAP codes as a result of its participation in the IDCOR program, for which Peach Bottom is a reference plant. The routine evaluation of risk at this level is not planned, but may be done when design features or procedures being analyzed are anticipated to have an effect on containment response or release quantity.

Types of Initiator: Internal Events - Another item involving the technical scope involves the assessment of internal initiators and external events. The internal initiators are more directly amenable to treatment, represent the more likely source of plant damage and are more likely to be affected by operating practices and modifications. The uncertainty associated with seismic and fire coupled with the overall reliance of these techniques on the base risk assessment models, suggest that they be delayed and possibly considered as a second priority set of events to be addressed. Fire represents the next level of interest beyond the Internal Initiators as plant practices may affect the initiating frequency. Higher uncertainty is associated with seismic risk due to the uncertainty of the seismic hazard curve and continuing through the
component response fragility. The major benefit of the external events
analysis results from the initial evaluation which has confirmed the adequacy
of the plant-specific design standards in this area.

Level of Detail: Current - There are no plans to change the level of detail in
the plant model. The current level is extensive and extends in most cases to
the point for which data exists. If model extensions are required for specific
studies, they will be incorporated into the model.

System Scope: Current - As with the level of detail, there are no specific
plans to extend the plant model to additional systems. However, it is
envisioned that issues related to plant availability, analysis of precursor
events and internal initiator frequency will result in additional models of
plant systems. As appropriate, these would be incorporated into the plant
model.

11.6 Organization
The establishing of technical bases and identification of potential
applications are relatively simple compared with the assignment of
organizations to accomplish the work. PECO's goal in this area is to gain
maximum impact from the continued PRA use in a manner which is compatible with
existing organizational philosophies and general responsibilities.

Philadelphia Electric Company's organization is functional with an Electric
Production Department focused on the immediate needs of operating and
maintaining the plant and an Engineering and Research Department devoted to the
technical support of operations, particularly the longer term, technically

Intensive activities such as design changes and studies. Within this
framework, no one location was found to be appropriate for a group which could
be both involved with normal plant operations and practices as well as being
dedicated to the technical aspects of PRA use. Consideration of the
establishing of a new group which would be independent of the existing
organizations led to the conclusion that a perception would be created that PRA
use and application of its concepts were "special" activities, not part of
normal work. This, of course, would be diametrically opposed to the intent.

The investigation yielded the conclusion that the interface between Electric
Production and Engineering was not a barrier to be overcome, but a well used
path for information exchange. Therefore, responsibilities for PRA application
have been assigned within each organization, and the associated interfaces have
become well defined. Within the Engineering Department, a group has been
established to deal with keeping the risk model up-to-date, maintaining the
capability to perform analyses using the model, analyzing modifications and
responding to requests for studies by Electric Production. Within Electric
Production, the Nuclear Safety Section has been identified as the appropriate
focal point. With Independent Safety Engineering Groups (ISEG's) at each
plant, they are intimately involved in plant operations with heavy
concentration in issues of plant safety. PRA applications are a logical
extension of their work in analyzing the safety impact of proposed actions and
reviewing activities at PECO and other Nuclear Power plants for areas of
improvement.
In summary, the organizational issue has been addressed by assigning responsibilities within the existing organization and using existing interfaces.

III. PROGRAM IMPLEMENTATION
To gain maximum benefit from PRA applications it is desirable to have Philadelphia Electric Company employees deeply involved in the effort, with consultant support limited to major efforts which require augmentation either for manpower or specific expertise. It is also necessary to have widespread knowledge of PRA concepts and insights so that these are reflected in normal work activities and that situations which warrant question or analysis are recognized. To address these factors, two important facets have been included in the PECO program.

III.A Technical Advisory Panel (TAP)
Although a number of PECO engineers were deeply involved in the performance of the Limerick PRA and have participated in PRA-related work through industry groups such as the Boiling Water Reactor Owners Group and IDCOR, there are many areas where specific expertise is lacking. To fill this void a Technical Advisory Panel (TAP) has been established to provide advice in system modeling, problem solving and methods of analysis. The initial three (3) panel members were selected based on their extensive knowledge of PRA and its applications as well as their involvement with the Limerick PRA. The TAP meets approximately quarterly to discuss recent and planned PRA work at PECO. It has proved to be a necessary adjunct to the continuing efforts.

III.B Training
A training program has been established to assure that the personnel involved with nuclear plant design and operations are sufficiently aware of PRA techniques, insights and applications. The program was developed in conjunction with the TAP and consists of three levels of training.

Overview Training
In a session lasting about one and one half (1 1/2) hours, PRA concepts, key insights, major results and potential applications are discussed. The thrust of the overview presentation is toward awareness by the audience which is primarily management and operations/engineering personnel who do not have direct involvement with plant systems.

Familiarization Training
This one day presentation provides expanded treatment of PRA concepts, insights and results. Although designed for engineering and operations technical personnel with system responsibilities, it is also attended by operations and engineering management from areas where PRA applications are particularly valuable. The focus is on how the PRA concepts and insights can be applied to the decisions which are made in the normal course of work.

Applications Training
In a two-day extension of the Familiarization presentation, selected personnel perform "hands-on" applications of the Limerick PRA such as operating experience review, analysis of a proposed modification or development of a procedure in small groups. The attendance is limited to those directly involved in PRA application, e.g., ISEG and PRA engineers.
In combination, the training program and the TAP assure that PRA awareness is widespread, PRA knowledge is concentrated where needed and that PRA applications are performed in a technically sound manner.

IV. SHORT TERM OBJECTIVES

Defining the initial tasks and establishing the necessary tools for work are significant activities. In order to assure that the proper attention is paid to the initial PRA activities, a Departmental Objective has been established within Philadelphia Electric Company's Management by Objectives framework. This defines the initial work scope, identifies the schedule for task completion and provides for periodic status reporting to upper management. The three major tasks in this Objective and the current status is listed below.

IV.A "As-Building"

The Limerick PRA is based on the plant design in the 1980-1981 time span. Since that time a large number of small design changes have been made, incomplete system designs have been completed and installed, final plant Technical Specifications have been issued and procedures have been written. The as-building effort will lead to a plant model which reflects these changes. The major items from the perspective of personal resources are as-building the system level fault trees and incorporation of the plant emergency procedures which implement the BEROG Emergency Procedure Guidelines (EPG's).

The fault trees from the original PRA have been reviewed by the responsible system engineers for comparison with the final plant design. Comments from the review are now being addressed or incorporated, after which the trees will be quantified, redrawn and circulated for final approval.

The original Limerick PRA was done before the BEROG EPG's were issued. Incorporation of the plant-specific procedures, therefore, is a new effort rather than just a review/update. This is a task which exceeds the manpower available at PECO and consultant assistance has been needed.

The as-building effort is scheduled for completion in September, 1986.

IV.B Training

The three level training program described above is an integral part of the Objective. The initial training target has been met with the first familiarization sessions being held in November, 1985. Training is expected to continue frequently through 1986, with periodic sessions thereafter.

IV.C Support Program

The final implementation step is the definition of specific roles for personnel directly involved in PRA use and identification of specific procedural changes which may be desired. Work is scheduled to start late in the as-building process with a final "Program Plan" being issued in September, 1986.

V. PLANNED APPLICATIONS

Resources are expected to be available for applications work as the efforts to baseline the PRA to the as-built plant are nearing completion. At this point, major initial efforts appear to be in the areas of Technical Specifications and analysis of plant equipment failure data.
V.A Technical Specifications

During the final stages of Limerick licensing some preliminary analyses were made of the risk sensitivity of the allowable out-of-service times (AOT) and surveillance test intervals (STI) for several systems. This indicated that appropriate values for Limerick might be considerably longer than those in the standard Technical Specifications. Since that time, PECO personnel have become more knowledgeable in this type of analysis through participation in BMRG activities and it is planned to make a more rigorous analysis to determine if Technical Specification changes are justified using the as-built plant model.

V.B Data Analysis

The long term program will certainly include a provision for review of equipment failure and repair data. Although the initial plant operation period is probably not representative of expected plant equipment failure rates, the establishing of a process of data review will be initiated early in the program to assure that the proper information is being collected and to identify the long term support requirements. The existing plant maintenance system is well equipped to generate the required information through its existing processes and procedures.

VI. ROLE OF PRA IN SAFETY ASSURANCE

The preceding information has discussed PECO’s use of the Limerick PRA without significant reference to safety assurance. In many cases, use of a PRA in support of an operating plant has been used synonymously with “Safety Assurance Program,” but there has been no generally accepted definition of the term.

Safety assurance must include the combination of all the things which the plant owner does to minimize the risk to the Company and the public from plant operations. Certainly, well defined areas such as Quality Assurance, training, maintenance practices and design procedures are part of safety assurance. However, there are many ill-defined factors, such as perceptions of management’s interest in minimizing risk, which may also have significant impact.

Within this broad area, PRA fulfills a particular role. Through widespread knowledge of PRA concepts, it allows general use of risk-related thought in normal activities. In some instances it permits a relative quantification of the risks of proposed actions as an aid in decision making. It does not, however, replace any of the other existing areas which have proved to be effective in safe, reliable nuclear power plant designs and operations.

VII. SUMMARY

The Philadelphia Electric Company plans for continuing the use of the Limerick PRA in support of Limerick design and operations provides an effective supplement to existing procedures and practices in assuring plant safety.

- Through emphasis on PECO personnel rather than consultants the knowledge gained and insights learned will be retained within the organization for maximum long term benefit.
- By including an extensive training program there will be broad understanding of concepts and insights, permitting risk-related decisions to be made as a normal course of work.
The integration of PRA use within the existing organization will maximize acceptance and benefits.

The technical bases are focused where the personnel have the most direct effect and the risk measure has the most direct impact on the company.

**Figure III.4-1**
LIMERICK GENERATING STATION
CORE DAMAGE FREQUENCY POINT ESTIMATES

<table>
<thead>
<tr>
<th>INTERNAL EVENTS</th>
<th>CORE DAMAGE FREQUENCY (PER REACTOR-YEAR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOSP</td>
<td>$6.6 \times 10^{-5}$</td>
</tr>
<tr>
<td>ISOLATION EVENTS</td>
<td>$3.0 \times 10^{-5}$</td>
</tr>
<tr>
<td>TURBINE TRIP</td>
<td>$8.1 \times 10^{-7}$</td>
</tr>
<tr>
<td>IORV</td>
<td>$8.5 \times 10^{-7}$</td>
</tr>
<tr>
<td>MANUAL SHUTDOWNs</td>
<td>$2.3 \times 10^{-7}$</td>
</tr>
<tr>
<td>AUXS</td>
<td>$1.2 \times 10^{-6}$</td>
</tr>
<tr>
<td>TRANSIENTS W/O CONTAINMENT</td>
<td>$9.6 \times 10^{-7}$</td>
</tr>
<tr>
<td>HEAT REMOVAL</td>
<td>$1.1 \times 10^{-7}$</td>
</tr>
<tr>
<td>TOTAL (INTERNAL EVENTS)</td>
<td>$1.5 \times 10^{-5}$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EXTERNAL EVENTS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>FIRE</td>
<td>$3.4 \times 10^{-5}$</td>
</tr>
<tr>
<td>SEISMIC</td>
<td>$5.7 \times 10^{-5}$</td>
</tr>
<tr>
<td>TOTAL (EXTERNAL EVENTS)</td>
<td>$0.9 \times 10^{-5}$</td>
</tr>
<tr>
<td>TOTAL (INTERNAL AND EXTERNAL)</td>
<td>$2.4 \times 10^{-5}$</td>
</tr>
</tbody>
</table>
Although there is general agreement that performing an uncertainty analysis as part of a PSA is desirable, there is little concensus as to how best to carry it out. In this paper we consider this question from the standpoint of the purposes of the uncertainty analysis.

There are two of these: the insight purpose and the decision purpose, with the second being viewed as an extension of the first. The insight purpose requires a philosophical and mathematical apparatus for the representation and propagation of uncertainty and a number of possibilities have been suggested, including: qualitative methods, classical statistical methods, probability methods, likelihood, bounds, generalised bounds or fuzzy set possibility, and finally a new method, which has been successfully applied to a recent analysis of CDFR, called the restricted bounds method. This combines the ease of eliciting bounds with a simple propagational mechanism to give insights which have turned out to be useful. Each of these methods has adherents and detractors and there seems to be no basis for deciding which is generally best suited to providing insights.

For making decisions there are two choices. Either use Bayesian Decision Theory, based on representing uncertainties by probability distributions, or one of the others. In the latter case a definite, but vaguely defined, degree of risk aversion is introduced. This may or may not be desirable depending on whether the decision lies in the safety or the economic domain. However, since there seems to be no rational basis for defining the decision parameters for other mechanisms, the standard decision theory approach appears to offer the best way forward.

Decision theory depends on probabilities and utilities which are subjectively assessed by comparisons with situations with known probabilities. Attitudes to risk are conventionally incorporated in the utility assignments but it is known that this does not adequately represent individual risk perceptions. In fact it is argued that the assignment of utilities for both economic and safety decisions may be relatively straightforward if attitudes to risk are incorporated in the assignment of the necessary subjective probabilities. Furthermore there appears to be no reason why non-probabilistic methods should not be used before the final probability assignment; indeed the best method may be the one which gives the best insights. Thus one is still left with a very difficult judgemental problem, but one for which the context may be better defined.

To be presented at the NEA CSNI PWS Workshop on PSA as an Aid to NPP Management held at Brighton, U.K., May 20-23 1986.
Introduction

One of the most difficult and controversial areas of PSA is uncertainty. It is a topic which on the one hand reaches into the philosophical foundations of probabilistic, or quantitative, safety assessment and on the other hand is of central interest to plant managers who wish to know whether and how PSA results can be used. The intention of this paper is to examine the purposes of uncertainty analysis and hence to see how the analysis can best be carried out to achieve the relevant aims.

It is possible to identify two basic purposes of a PSA uncertainty analysis. The first (insight purpose) is to understand the PSA better and to gain a better grasp of its limitations. The other (decision purpose) is to enable decisions to be made; it seems intuitively clear that an output risk to be compared with a safety goal is useless without some kind of error bar, or some more subtle interpretation of the output. This point has been strongly made by Holloway (Interpretation of PSA Output for Safety Decisions, IAEA workshop, Budapest, October 1985) who contrasts decision-making subject to (PSA) revealed uncertainties with decision-making subject to unrevealed uncertainties. He shall discuss both purposes but shall concentrate for the most part on the requirements of decision-making since this will be of greater interest to this Workshop.

The insight purpose requires the generation and manipulation of information in a way which is acceptable and useful whereas the decision purpose requires additional philosophical and mathematical apparatus to construct a mapping of this information into the binary (yes, no) set. This additional content is what we shall largely be concerned with, but we need to point out that, although it is plausible that the same machinery which is used to fulfil the insight purpose should be extended for the decision purpose, this assumption should be subject to critical examination.

In the following sections we shall describe firstly various methods which can be used to represent uncertainty and then consider how they may be extended for decision-making purposes. However, a useful preliminary is to consider in more detail what is required to fulfill the insight purpose. PSA is concerned at a fundamental level with a process of frequency estimation and what we want to do is to form a view as to the values these estimates could reasonably take in the light of the (limited) data available. It is desirable that this should be done in a way that is clear, repeatable, resilient, useful, philosophically respectable and non-controversial. Simplicity and ease of calculation are also preferred properties.

It also needs to be borne in mind that the data available for doing this will be of various types. The simplest situation is that of statistical data, for example failure data for a particular component, in which case there are accepted statistical techniques available. However, a much more difficult problem arises when the experimental evidence is of doubtful relevance and there is insufficient modelling expertise such as is typically the case in analysing the effects of degraded core accidents. This is sometimes referred to as the data-free case though this is erroneous since the situation is simply that the ne-
ture of the data is different. The relevant parts of the PSA are still based on data even if, for example, this is the intuitive expertise of an experienced engineer. Making PSAs controllable depends in part on starting as completely as possible the entire database used, whether it be processed objectively or subjectively.

Considering further the analysis of non-statistical data, a typical PSA technique is to assign probabilities to the nodes of an event tree. The nature of most of these probabilities is not the same as that of a coin landing heads. In practice the event of interest either will or will not occur in a given set of circumstances so that the true probability is 0 or 1, the assignment of other probabilities is in fact a reflection of our uncertainty about the process. Thus it could be argued that it is not meaningful to investigate uncertainty further by varying the values. This is particularly true of the approach which uses probability distributions to represent uncertainty in a parameter since if the two probabilities (the estimate and the probability distribution thereon) are treated on an equal basis, the only meaningful result is the expectation value. We sidestep this criticism, however, by arguing that the PSA method is to estimate frequencies using event tree quantifications. If now the purpose of the uncertainty analysis is to investigate what other values the estimates might reasonably have had in the light of the incomplete data available, we have to confront alternative values in the quantification. To put it another way, we are trying to define the set of PSAs which would be acceptable.

In Section 2 we shall describe various means of representing and propagating uncertainty. This will be done briefly since it forms the topic of a previous paper (Assessment and Presentation of Uncertainties in Probabilistic Risk Assessment, IAEA Seminar, Blackpool, March 1985) though we shall enlarge on one new method. Following this, Section 3 is devoted to examining how decisions can be made on the basis of these methods. In Section 4 we examine how our findings relate to the usual formulation of decision theory and finally our results, conclusions and recommendations will be described in Section 5.

2 Ways of Representing Uncertainty

The USNRC Procedures Guide (NUREG-CR-2300) proposes the use of qualitative and quantitative uncertainty analyses. Starting with the first of these, a qualitative analysis consists of a list of sources of uncertainty together with a subjective assessment of the importance of each. Naturally this assessment should bear in mind the particular result which will be used.

The first quantitative method is that of statistical confidence bounds. For example, an upper 95% statistical confidence bound on the failure rate of a system has the property that, whatever the true rate, the bound will exceed it with probability at least 0.95. The advantages of this approach are: construction of bounds is very difficult, even for quite simple cases; it is not obvious how the method could be extended to situations where the data is not in statistical form; it is not clear by how much the probability exceeds the confidence level (95% in the above case) as a function of failure rate.
Probability methods represent uncertainty in a particular parameter by means of a probability distribution. For cases involving statistical data a subjective prior can be updated using objective likelihoods by means of Bayes' Theorem. For other types of data a structured approach could use an updating process with subjective likelihoods or the probability could be subjectively assessed at the outset. Alternatively, probability distributions can be derived using maximum entropy methods from other types of information (Cook and Uwini, Principles for Prior Probability Assignments, NUREG/CR-4514, February 1986). Once the distributions are available it is straightforward, in principle, to derive the relevant distribution for any output parameter. The most important objection to this approach is that there is too much subjective input, with corresponding unpredictable effects on output. Other disadvantages spring from the measure theoretic nature of probability such as the difficulty in satisfactorily representing total ignorance (and thus, by implication, partial ignorance).

These measure problems are overcome by methods which assign degrees of belief pointwise. These will have different propagational algebras from probability methods which may be intuitively more appealing. Edwards (Likelihood, Cambridge U.P., 1972) criticises the application of statistical and probability methods and suggests the use of likelihood. The essential difference between likelihood and probability lies in their propagation: the likelihood of a particular value of system reliability, say, is the maximum likelihood of all possible component reliability combinations giving that reliability. That is, an output value is disbelieved only to the extent that all input value combinations leading to that output are disbelieved. For inferences about systems based on statistical data, likelihood appears to form a useful measure of uncertainty, indeed many methods of generating statistical confidence bounds rely on calibrations of likelihoods. In the absence of statistical data there seems to be little to choose between subjective likelihoods and subjective probabilities, except that likelihood can represent total ignorance. One disadvantage of likelihood is that it is a more unfamiliar concept, particularly with regard to its operational definition.

A method which some consider to have less subjective input in situations where statistical data is not available is the use of bounds. Experience suggests that uncertainty information is often most easily elicited in this form and it is straightforward to combine input bounds to produce overall output bounds. One can attach various interpretations to bounds, for example, defining them such that the excluded values can be shown to be unreasonable. The same interpretation would then attach to the output bound, though probability minded people object that combinations of improbable input values lead to very improbable outputs so that an inferential inconsistency is introduced. It can also be argued that discontinuous degrees of belief, as implied by the bounding approach, are unrealistic.

A generalised bounds method can be devised by attaching degrees of belief to input parameter values and propagating each level of belief as a bound. This point method has some of the same propagational properties as likelihood, and in fact propagates in the same way as possibility derived from fuzzy set concepts (Dubois and Prade, Fuzzy Sets and
Systems). A high degree of subjective discrimination is needed to apply this as in the case of probability and likelihood.

Finally a brief description is given of a new method, the restricted bounds method, which has been used to represent information in the recent CDFR PSA (Abbey et al., CDFR Risk Assessment, Fast Reactor Conference, Guernsey, May 1985). This takes what seems to be a very practical approach of eliciting the uncertainty information in the form of bounds (about so-called best estimate values which are used elsewhere in the PSA) and then observing how the output values change as the input parameters vary between their bounds. This is done by imposing successively the restrictions that only one input probability at a time may vary, than two, than three, and so on. The output uncertainty information is then the maximum and minimum values of the output frequency obtained when all possible combinations of the allowed number of input probabilities are varied between their bounds. The name of the method derives from the fact that we are restricting the number of variables which can vary from their best estimate values. The results of a particular calculation where $n$ of the inputs are allowed to vary are then termed restricted bounds of order $n$.

In the case that $n=0$ we obtain the best estimate output frequency, and in the limit that $n$ is equal to the total number of input variables we recover the normal bounding analysis described above.

An interesting by-product of this method is that it allows a ranking of the input parameters by importance for uncertainty. This is achieved by observing which one gives the maximum variation. This information is then useful in deciding how best to reduce uncertainty.

If we compare the restricted bounds method with the checklist of desirable properties contained in the previous section we find: it is certainly clear in itself and easy to follow in practice, it is easily accessible to scrutiny, its replicability depends on the replicability of the bounds, a question we do not address, but is otherwise easy, we believe that it gives useful insights as to what output values are reasonable, the stated aim of the insight purpose, its philosophical content is small, apart from the definition of bounds, a problem common to all methods exploiting bounding ideas, nothing in this area is uncontroversial; it is undoubtedly simple and easy to calculate.

In practice, the restricted bounds method appeared to be useful way of representing information, with the particular advantage that other types of uncertainty beyond what is normally included in a quantitative analysis can be considered. An example is the uncertainty resulting from grouping accidents together for the estimation of source terms.

We can summarise this section by observing that there is little consensus as to how uncertainty should be represented and propagated. People are attracted differently by the various advantages of each method and presumably this reflects a fundamental difference in how they can best appreciate the information available. As far as the insight purpose is concerned, there seems to be little more to be said, so let us turn to decision making.
3. Making Decisions

In this section we shall discuss how the methods described in the previous section can be extended to provide decision making algorithms. We shall illustrate each method with two standard examples:
- deciding if a plant meets a safety goal defined in terms of a risk target, and
- deciding if a proposed plant modification is cost effective with regard to increased availability.

Halloway argues that in the PSA field there is little innate understanding of the uncertainties such as is used to make decisions in other areas. A qualitative uncertainty analysis is a first attempt to represent what innate information exists in a systematic way. However, it does not offer a guide as to how decisions should be made.

Making decisions on the basis of statistical confidence bounds is called hypothesis testing. For example, a plant would be deemed safe enough if the upper confidence bound on risk at some (high) confidence level were less than the target. Thus two parameters have to be defined: the goal and the target. Note, too, that a lack of reversibility has been introduced: the null hypothesis is "the plant is not safe enough" and it is rejected only if we are confident there is enough evidence to do so. Thus an element of risk aversion has been introduced, both in the null hypothesis and in the high confidence necessary to reject it. This is considered appropriate, even desirable, for a safety issue, but it is not clear how to define a decision algorithm for the plant modification problem which has no safety connotations. We know that the break-even reliability will be but not what confidence bound it should be compared to (not forgetting that the 50% upper confidence bound will most likely differ widely from the 50% lower confidence bound).

These problems disappear when probabilistic methods are used. Using Bayesian Decision Theory one simply sets up a subjective prior distribution on the reliability, updates it in the light of the data, calculates the expected loss from the two decision choices and decides on the one with the smaller expected loss. This process is eased because the losses due to poor reliability are relatively easily calculated on the same scale - money - as the cost of the modification. In decision theory jargon, the utility of the possible outcomes is straightforward to calculate. The problem which immediately arises for the safety decision is partially solved if one is deciding whether a risk target has been met though it is still necessary to define utility as a function of risk with the property that it will be negative for risks exceeding the target and positive for values less than it. Using the "natural" linear assumption the condition for acceptance is simply that the expected risk be less than the target.

If now, as is usual, it is desired to introduce an element of risk aversion for the safety decision, the standard decision theory method is to make appropriate adjustments to the utility function. This would require breaking the risk down into the various consequence levels and assigning a proportionately larger disutility to high consequences. As a result the safety goal would no longer be a pure risk. There are two obvious alternatives. In analogy with statistical confidence bounds
we could define Bayesian confidence bounds. This would correspond to placing a constant utility with much larger negative value above the risk target than the positive value below it. Alternatively, some other utility function in terms of risk could be defined, such as the square, which would lead to more restrictive targets than with linear utility, but in a rather uncontrolled and unclear way. We shall return to decision theory in more detail in the next section.

In his book, Edwards says very little about what values of likelihood should be adopted for decision making purposes. As in the case of statistical confidence bounds, selecting a value other than one indicates a degree of risk aversion. This may be useful for the safety decision but is not easy to interpret. For the economic decision there is no obvious reason to be risk averse so one would look at the maximum likelihood reliability estimator, which amounts to ignoring the uncertainty analysis.

Similar remarks apply if simple bounding, generalised bounding or restricted bounding methods are used. If the uncertainty information is incorporated into the decision making process in the obvious way there is definite, but vaguely defined, risk aversion implied.

This leaves the decision maker a clear choice: either to use probability methods and decision theory or to decide on the basis of one of the other methods, incorporating his attitude to risk as necessary, but relying on his intuition and understanding of the PSA as evoked by the insight function of the uncertainty analysis. Of course, this latter course is subjective and lacks scrutability but it may be that if the insight purpose is sufficiently well carried out (using, perhaps, the restricted bounds approach described earlier) these disadvantages will be outweighed by the more hidden effects of defining and propagating subjective probabilities.

In the long term, however, the decision theory approach appears to be preferable and in the next section we examine some aspects of this in more detail and what implications this has for the uncertainty analysis.

4 Decision Theory

We have seen that there are two underlying themes to the problem of decision making using PSA results with revealed uncertainties. One is coping with subjectivity and the other is attitude to risk. We begin by observing how these are conventionally tackled in decision theory.

Lindley (Making Decisions, Wiley, 1985) shows that the only logical way for the coherent decision maker to proceed is to maximise expected utility. The proof depends on forcing his to assign preferences to various gambles with known probabilities to determine a subjective utility function, and likewise to determine a subjective probability where appropriate in the same way. This apparently rules out any other approach, except that he goes on to say that this applies only to a single decision maker and that the problem is unsolved for multiple decision makers. Apart from the technical problem of decisions being made by committees or other groupings, this underlines that fact that subjective probability methods rely (in general) on the subjective assignments
of one person (the assessor) being used to make decisions by another. It needs to be emphasised at this point that this approach is aimed purely at defining how decisions should be made rather than describing how they are made.

Now the emphasis of this argument is on defining a utility function: anyone who accepts known probability gambles in a way which is inconsistent with maximising expected utility for some utility function can be said to lose consistently. This is the nature of the proof. But of course the same is not true of gambles (such as the decisions we are concerned with here) for which the probabilities are not known and must be subjectively assessed. Consequently the theory remains silent (or nearly so, see below) on how to assess these.

The conventional way to incorporate attitude to risk in decision theory is by appropriate utility functions, but it is actually plausible to separate two effects: attitudes to high consequences (to be incorporated in the utility) and attitudes to randomness (to be incorporated in the probability assignments). There seems to be no reason why this should not be done for both decision problems of the previous section.

This leads to the point that defining a universally acceptable utility should not be as difficult a task as is sometimes thought since the attitude to randomness can be put on one side. For economic decisions the normal utility of money would be appropriate whereas in the safety field it may be appropriate to propose disproportionately large disutilities for large consequences, though there are also arguments against this. Munera (The Generalised Means Model for Non-Deterministic


Once a utility function has been agreed the decision theory requirement to assign subjective probabilities becomes a truism since any decision, once taken, is equivalent to setting a probability bound. We thus have to arrive at a means to carry this out. To fix ideas, consider the two following alternatives:

- the certain knowledge that a dice is rolled every second and some accident occurs when 12 successive sides turn up, and
- the result of a PSA is that the accident frequency is 5.2(8) per year.

Although the risks are arithmetically the same, the risk perception of each of these is likely to be different and our attitude is likely to differ for the economic as well as the safety decision. The function of the uncertainty analysis is to provide help in resolving the problem. It can be seen that the outstanding questions of subjectivity and attitude to risk have more or less cascaded into a single problem.

The decision theory approach, as exemplified by Lindsey's book, carries the clear implication that the only correct approach to uncertainty of all kinds (rather than that immediately involved in the decision) should be represented by subjective probabilities. This is based on overall coherence and the opportunity to use Bayes' Theorem to structure probability assignments. However, there is no mathematical proof that someone who bases his decisions on probabilistic uncertainty ana-
lyses enjoys a consistent advantage over someone who uses another method and we have in any case pointed out that the safety assessment process cannot incorporate a single person’s subjectivities. Thus, it does not follow that the complete uncertainty analysis needs to be done using probabilistic methods. There seems to be no reason why these probabilistic methods should not be assessed prior to the decision by using, say, the output from a restricted bounds analysis. Of course it is not possible to provide a prescription for doing this but it is in the very nature of subjective assessment that this is a reasonable proposition. This is underlined by repeating our suggestion in the Introduction that the methods which best fulfill the insight purpose may well form the best starting point for the decision purpose.

5 Conclusions

The intention of this note has been to set out the purposes of PSA uncertainty analysis and hence see what methods can best be used to achieve this purpose.

The two identified purposes are to gain insights (both into the safety of the plant and the application of the PSA) and to aid in decision making.

We have briefly examined some of the many methods proposed for representing and propagating uncertainty including a new method, the restricted bounds method, which has proved useful in carrying out the quantitative uncertainty analysis in the recent CDFR PSA. It is clear from the range of these methods, and the vigour with which each one is defended, that there is no consensus on how best to achieve useful insights and that this question cannot be answered for the time being.

Turning to the implications of each method for decision making, it becomes clear that, with the exception of probability methods, there is no systematic way of incorporating the uncertainty analysis except by the application of a rather undefined degree of risk aversion. This may be appropriate for safety decisions, but is not for purely economic ones. In addition it seems reasonable that attitudes to subjectivity and risk should be better defined.

In the light of this we examine further how decision theory techniques based on subjective probabilities and utilities can be applied. We suggest that it may be easier than is generally thought to arrive at universally acceptable utilities for both economic and safety decisions and this aligns well with the coherence requirement of decision theory. In contrast, the assignment of probabilities contains the difficult subjectivity and risk perception problems and it seems neither logically nor practically necessary to follow the decision theory approach of representing all uncertainties with subjective probabilities. In fact it is tentatively proposed that the method which best fulfills the insight purpose may be of the greatest help to the decision maker.

It is thus recognised that the questions which we intended to attack remain unanswered, but it is hoped that this material can provide a useful starting point for further discussion within the Workshop.
1. INTRODUCTION

The output of Probabilistic Safety Assessments for Nuclear Power is often presented as a single frequency, for example the frequency of core melt. To be of value in supporting safety cases for the acceptability of the design this point value should represent a mean value or a value on the pessimistic, rather than optimistic side of mean. Undue pessimism is to be avoided as it may lead to a distorted and uneconomic design.

A mean frequency for core melt is obtained from Event and Fault Tree analysis which uses mean data for initiating Event frequencies and component failure rates. There is however a variability associated with component failure rates, arising from such factors as manufacturing tolerances and variations in operating environment, which can be represented as a probability density function (pdf). The term uncertainty is sometimes associated with this variability. (There is also uncertainty in the derivation of the pdf which is associated statistically with the necessity to sample a limited number of components; the discussion in this paper is not concerned with this source of uncertainty.) The probability density distributions for each of the variables in a PSA can be combined in the analysis to yield a probability density distribution for the overall answer. In practical terms this means that whereas the mean frequency of core melt of a plant of given design might be $10^{-5}$ p.a., one plant in a hundred might have a core melt frequency of $10^{-3}$ p.a. and one in a hundred $10^{-7}$ p.a. In section 2 the derivation of mean and median values for the result of a PSA is discussed. Relationships between the median and mean are derived and examined assuming a log-normal distribution of component reliability. Section 3 discusses the implications of section 2 for the practical value of predictions of uncertainty in the outcome of PSA.

The ability of safeguards systems, to prevent core melt for example, is justified by transient analysis. Predictions of parameters such as fuel clad temperature also have associated probability distribution functions which can be derived if the probability distribution functions of all relevant input parameters are known. In general transient analysis is carried out using conservative values of input parameters so that the probability of limiting design criteria being exceeded in a given transient can confidently be said to be small compared with the probability of failure of operation of the safeguards systems assumed in the analysis. Section 4 explores the implications of predictions of uncertainty in the results of transient analysis, arising from the uncertainty associated with the input variables, for the methods and predictions of PSA.

It is argued in this note that predictions of uncertainty of the results of a PSA are of no value to the designer or assessor of NPP. Predictions of uncertainty associated with the outcome of transient analysis can however be argued as if it is feared that unnecessary pessimism is unduly distorting the design. It is nevertheless acknowledged that there may be in some circumstances unquantifiable uncertainty in the mean values of component reliability, and appropriate measures in recognition of this are suggested in section 5.

2. THE PROPERTIES OF PROBABILITY DISTRIBUTION FUNCTIONS

It is implicit in the definition of the mean of a pdf of a probability or frequency that it involves integrating over the whole range of probabilities of the occurrence of the probability or frequency in question.

Thus if nine plants in ten of a given design have a frequency of core melt of $10^{-6}$ p.a. say, and one in ten has a frequency of $10^{-9}$ p.a. then the mean frequency is approximately $2 	imes 10^{-6}$ p.a. If on the other hand one plant in ten has a frequency of core melt of $10^{-6}$ p.a. then the mean frequency is approx. $10^{-5}$ p.a. whereas if the tenth plant has a frequency of core melt of $10^{-7}$ p.a. then the mean is approx. $10^{-6}$ p.a.

It can be shown that if mean values of all input component failure probabilities are used then the computed value of the fault tree top event probability is also the mean value. If the probability distribution functions of the component failure probabilities are symmetric (and have a single peak) then median (and mode) values will be the same as the mean. In general however the probability distribution function is skewed and a log-normal distribution has been found to be a useful assumption. This assumption enables the variance in component failure rates to be expressed as a range factor. For the log-normal distribution the mean value is greater than the median, the difference being a function of the variance (see Figure 1).

If median values are used for the individual component probabilities, or for the values of input variables to transient analysis, then it is often assumed that the calculated and point of the analysis will also be the median. This is not strictly true but may be an adequately accurate assumption. If 95% confidence limit values are used then greater than 95% confidence is obtained for the result.

It should be acknowledged that Lewis (Ref. 2) in his review of the Reactor Safety Study (Ref. 1) criticized Rasmussen for not making clear that median values of component reliability rather than means were being used.

Given that complete probability distribution functions are known for the input variables, then a complete distribution function and in particular the mean, the median and 95% confidence limits (or any other interval) can be derived. Techniques are available to do this, but the amount of computation involved may make the task infeasible.

To summarise, if it were feasible to obtain rigorously the median value for the end point of a PSA, then one can say that the result will be exceeded by just 50% of plants of that design. The mean result of a population of plants, or the expectation value for a single plant will in general be higher than the median value. The only way to ensure that a mean value is obtained is to use mean values for the input data.

In section 3 the meaning of predictions of uncertainty in reliability analysis is discussed.
THE USE OF PREDICTIVE OF UNCERTAINTY IN PSA

by M H Lee
Central Electricity Generating Board
Generation Development and Construction Division

ABSTRACT

The results of PSA may be presented as a single value for the frequency of, for example, core melt. There is an uncertainty associated with this value which is a consequence of the uncertainty in the initiating Event frequencies and the component reliability data arising from factors such as manufacturing tolerances and variations in operating environment.

It is often asserted that it is important to know the uncertainty in the results of PSA and that a plant with a lower uncertainty is to be preferred to a plant with the same mean value but a higher uncertainty.

This paper examines the practical implications of the use of median and mean values in PSA and concludes that mean values should always be used and that if this is done predictions of uncertainty have no practical value.

To be presented to the CSNI Workshop on PSA Support to NPP Management, Brighton, May 1986.
Where there is uncertainty about the actual reliability of a type of component, rather than about an individual component within that type, then sensitivity studies should form part of the PSA to indicate the significance of the uncertainty. For significant components appropriate measures are taken in design and operation to ensure that adequate reliability is achieved.

ACKNOWLEDGEMENTS

This paper is published by permission of the Central Electricity Generating Board.

This document expresses the personal views of the author and does not commit the CEGB to any policy or statement written into or inferred from the contents.

REFERENCES

3. THE MEANING OF THE PROBABILITY DISTRIBUTION FUNCTION OF A FREQUENCY OF AN OCCURRENCE

From the probability distribution function for the frequency of core melt of a particular design one can deduce for example that one plant in twenty might have a core melt frequency greater than a certain value, or that there is a 3% probability that a given plant will have a core melt frequency greater than that value. It might intuitively be expected that the 'risk' from the plant is dominated by the 3% probability of it having a core melt frequency in the upper tail of the distribution, and is in fact higher than the mean. This cannot be the case since the mean is obtained by integrating over the complete probability range from 0 to 1 and must therefore be greater than the integral over some portion of the range. If the mean value obtained from PSA is acceptable then no must the 95% confidence limit also be.

An argument put forward for the value of prediction of uncertainty is that a design having a certain mean frequency of core melt and a low variance, or spread, or uncertainty about this mean is to be preferred over a design with the same mean but higher uncertainty. From the discussion in the previous section it can be deduced that the design with the lower spread will, apparently paradoxical, have a higher median value (see Figure 2).

The apparent attraction of the plant with low spread may be a result of risk aversion. The possibility of a high frequency of core melt, albeit at a low probability, is viewed unfavourably but illogically in a similar way to the aversion to a low probability of a high number of deaths compared with the same overall risk for a smaller number of deaths.

It is the author's view that criteria can be developed to reflect society's attitude to risk aversion. PSA's would be compared with the criteria but uncertainty, as discussed so far, in the predictions of PSA would still be of no value in judgements on the relative acceptability of designs.

Unfortunately the designers or operators of nuclear power plant are not always, or even in general, completely certain about the mean or the distribution of the reliability data of their plant. Often this uncertainty is unquantifiable. Practical steps which should be taken in design or operation in recognition of this uncertainty are discussed in Section 5. In the next section however we discuss the value of predictions of uncertainty in the response of the plant.

4. THE VALUE OF PREDICTIONS OF UNCERTAINTY IN PLANT RESPONSE

PSA's are carried out to various levels ranging from an assessment of the frequency of exceeding design basis limits for the barriers to release to an assessment of the frequency of a range of health effects. Predictions of the outcome of fault sequences are derived from transient and radiological analysis embodying conservatism overall. The frequency of the fault sequence is obtained from Event and Fault Tree analysis. A rigorous PSA would require an assessment of the full range of outcomes of each fault sequence as well as an assessment of the whole range of fault sequences. In practice the amount of transient (and radiological) analysis required makes the approach unfeasible. Instead the analysis required to justify the interpretation of data which form the basis of Fault Tree analysis employs deliberate additional conservatism to cover more frequent fault sequences in which more than the minimum safeguards system equipment operates.

To satisfy the CEBG's Design Safety Criteria (Ref. 3) the confidence required of transient analysis for Fault Sequences of frequency of order 1 p.a. is of the order $10^{-7}$ or less. A rigorous demonstration would require calculation of the full probability distribution function of the output variable of interest (e.g. fuel clad temperature). This requires a knowledge of the pdf's of the input variables and because of the non-linearity of the response of the system a large amount of computation. In practice of course judgements are made on bounding values of parameters and on conservative physical modelling to achieve the required degree of assurance.

Bounding assumptions in the modelling of low probability fault sequences can lead to a definition of safeguards system requirements (i.e. minimum success criteria) which is more onerous than necessary. The effect is to make it difficult for the designer to meet the probabilistic targets he may be working to. Alternatively the introduction of additional equipment may lead to a plant which is more complex and hence perhaps less safe eventually as well as being more expensive. This situation may be avoided if lower confidence is sought from the outcome of the transient analysis.

Predictions of uncertainty in plant response can therefore be of considerable value to the usefulness of PSA in supporting safety arguments.

5. PRACTICAL STEPS TO BE TAKEN IN THE FACE OF UNCERTAINTY IN PLANT RELIABILITY DATA

In section 3 it was acknowledged that in practice there is in general some uncertainty about the nature of the probability distribution functions of the reliability data. This is particularly true when new designs are being developed.

The significance of lower reliability than assumed in PSA for any particular component can be obtained from sensitivity studies. Importance functions for components identify which components should be given most attention. Particular emphasis can then be placed at the design stage in procuring components of the required reliability and during operation in ensuring that maintenance and testing ensure that the desired reliability is achieved. In this sense proven components whose reliability is more certain are to be preferred to unproven components. The proper way to represent this uncertainty in the analysis is to bias the data for unproven components where this is based on that for the nearest equivalent proven component. Analysis of the data to establish the causes of poor reliability enables steps to be taken to ensure that components have a better mean reliability than that of the data used.

6. CONCLUSIONS

It is argued that in calculating and presenting the results of PSA only mean values should be used. The range about the mean is of no meaning or value in making judgements on the acceptability of a design.

Predictions of uncertainty in the outcome of transient analysis are however of value in ensuring that adequate conservatism is employed in defining safeguards system requirements. Excessive conservatism which may distort the design can be avoided.