THE 4TH INTERNATIONAL TOPICAL MEETING ON
NUCLEAR THERMAL HYDRAULICS, OPERATIONS AND SAFETY
April 6-8, 1994, Taipei, Taiwan

OBSERVATIONS ON PRA AND ITS APPLICATIONS

Yean-Chuan Yeh and Shoei-Long Shieh
Atomic Energy Council
67, Lane 144, Keelung Rd., Sec. 4
Taipei, Taiwan, ROC
Fax: 886-2-363-5377

ABSTRACT

An overview on the experience of PRA and its prospective application in Taiwan's three nuclear power plants is presented. Through the PRA, plant design improvements are performed and several engineering findings are illuminated. The sensitivity study including the internal, seismic, and typhoon events are conducted to justify items that can significantly reduce core meltdown risk. Its resulted plant betterment plans are thus highlighted accordingly. For PRA application, a risk-based inspection program for allocating inspection human resources has been resulted following the importance ranking of each component. The developing risk-based regulation to rationalize technical specification and maintenance program will also be entailed. To enhance the accuracy of the PRA model and its reproducibility, several issues are considered to have high priority for improvement such as external event data and analyses, uncertainty, common mode failure, human reliability, and the relative component importance. Highlight of their significance along with some typical sensitivity analyses are discussed for further investigation.

I - INTRODUCTION

Since the Reactor Safety Study, various organizations and individuals have recognized that the performance of a probabilistic risk assessment (PRA) enhances the understanding of plant design, operation, and the contribution made by each to the risk associated with operating the plant. This paper attempts to highlight the lessons learned and engineering insights resulted from the three nuclear power plants (NPPs) in Taiwan. The Chinshan NPP is a GE BWR-IV with Mark-I containment; Kuosheng NPP is a GE BWR-VI with Mark-III containment; and the Maanshan NPP is a Westinghouse 3-loop PWR with large dry containment.

The probabilistic risk assessment of the nuclear power station was carried out to determine the likely frequency of core melt accidents, its magnitude, its composition, and the associated frequency of fission products released in these accidents. This was achieved by dividing the analysis into two major parts. In the first part, all the possible failures and events that can cause the reactor transients or lead to a loss of coolant accident (LOCA) from the system were identified along with the designed response of every systems which can be used to maintain inventory within the reactor vessel and to remove the decay heat. The failure of certain systems to perform these specified function will eventually lead to a loss of cooling and results in core damage. In this PRA the onset of core damage is usually called core melt although there will be a period of time from the onset of core damage to completely melt the core and to become uncoolable within the vessel. This part of the analysis is called the system analysis and the results are a determined core melt frequency (CMF) and a description of the sequence of events which are most likely to lead to core melt during the plant's life. These events involve the initiating events, subsequent system failures, and incorrect operator actions. The possible recovery actions are also considered. The essential feature of this portion of the work is the development of a comprehensive model of the plant system, accounting for their dependency and interaction, and the normal and emergency operating procedures used by the operators. Quantification of these models incorporates failure data, which is as accurate as possible, in order to be able to determine the frequency with which events are likely to occur.

In the second part of the analysis, what to happen within the vessel and containment following the core melt accident is investigated. First a computer model is used to predict how the core melt will progress and how the core debris will interact with, water in the lower part of the vessel, the vessel lower head, on the drywell floor, and the concrete floor itself. The next stage is to determine how the resulting steam and hydrogen will behave inside containment and the pressure rise that may result if sufficient hydrogen is generated for a hydrogen burn to occur. In parallel with this work, the structural design of the containment is investigated to determine the likely failure rising pressure that may be caused at the various identified failure locations such as the personnel hatch, equipment hatch, penetrations or the dome. The results of these two branches of the work are combined to predict the probability of containment failure. Similar work is also performed on drywell to predict the probability of suppression pool bypass.

II - CMFS AND ENGINEERING INSIGHTS FOR PLANT-SPECIFIC PRAS

On account of slightly different analyzing methods to be employed, the initiating events are divided into two groups - internal and external. Internal initiating events are those directly associated with plant components or specific operator actions while running a test, for example, causing the turbine to trip or main steam isolating valves to close. Loss of off-site power, although external to the plant, is considered in this category as it has a direct impact on a specific system (power distribution) and elicits a clear cut response from the emergency diesel generators. External events are those whose occurrence results in failure of a number of components either as the result of environmental impact (fire or flood) or a common susceptibility to the external event (earthquake or typhoon). Thus, a flood caused by a system within the plant (such as the circulating water system) is still treated as an "external" event because of the impact of the flood can have on a number of apparently unrelated systems.

This section summarizes the analyzed results of overall core melt frequency, the events that lead to the dominant core melt sequence, and the significant failures for each sequences. The total CMFs for Chinshan, Kuosheng, and Maanshan NPPs are 1.4E-04, 9.6E-05, and 1.1E-04 per reactor-year respectively. Table I shows the detailed breakdowns of the relative contributions from the internal and external initiating events. Table II lists the relative contribution of internal initiating events.

Table I - Comparison of Core Melt Frequency for the Three Nuclear Power Plants

Contributor	Core Melt Frequency (1/R-Y)		
	Chinshan	Kuosheng	Maanshan
Internal Event	6.1E-5	1.4E-5	3.7E-5
Seismic Event	6.3E-5	5.3E-5	3.6E-5
Typhoon	8.8E-8	1.0E-5	2.8E-5
Fire	1.4E-5	1.8E-5	1.2E-5
Flood	1.4E-7	5.5E-7	3.5E-7
Total	1.4E-4	9.6E-5	1.1E-4

Table II - Contribution of Internal Initiating Events for the Three Nuclear Power Plants

Contributor	Percentages to Interanl Events		
	Chinshan	Kuosheng	Maanshan
Transients	17	19	13
ATWS	8	65	14
LOCA	5	6	30
Station Blackout	70	10	38
Loss of CCW	-	-	5

II.1 - Chinshan PRA

The core melt frequencies for Chinshan NPP resulted from internal initiating event, seismic event, typhoon, fire, and flood are $5.2X10^{-5}$,$6.3X10^{-5}$, $8.8X10^{-8}$, $1.4X10^{-5}$, and $1.4X10^{-7}$ respectively. The point estimate total core melt frequency is 1.4×10^{-4} per reactor-year. To the total core melt frequency, 44 percent is contributed by the internally initiated sequences, 46 percent by the seismically induced sequences, about 10 percent resulted from fire, and less than 1 percent from typhoon and flood.

For internally initiated sequences, the core melt frequencies are shown by the initiating events of LOCA, losses of off-site power, compressed air, and feedwater, feedwater trip, and other general transients. Each initiator can be followed by failure to scram and thus an anticipated transient without automatic scram (ATWS) is not strictly a separate class of initiating event. However, since the responses following an ATWS are similar, and since they are very different from those in non-ATWS situations, it is convenient to list them as a separate group. Loss of offsite power contributes 72 percent of the internally induced core melt frequency. To internal initiating events, general transients contribute 85 percent; LOCAs, 6 percent; and ATWS, 9 percent to the internally initiated core melt frequency.

Following engineering insights are considered to be sensitive to overall plant safety upgrade.

- Upgrade seismic susceptibility of control room ceiling;
- Upgrade seismic susceptibility of safety relieve valve accumulators;
- Install an independent (including supporting system) diesel generator;
- Install alternate rod insertion system;
- Install fire barriers to train A cables in fire areas 2G and 4D.

Other areas that are worth improving are the reliability of gas turbines (for offsite power recovery), the reliability of compressed air system (cross-tie to other unit), operator responses in mitigating ATWS, prevention of setting local valves of standby liquid control system in the wrong configuration, and mis-calibration preclusion of low pressure injection permissive signal.

II.2 - Kuosheng PRA

The task in the PRA for the Kuosheng NPP was two folds: estimate of the CMF and associated engineering insights into plant operation and safety. The methods of analysis was based on some conservative generic data. The original estimated CMF is $3.4X10^{-4}$ per reactor-year. Accordingly, a betterment program along with some plant-specific evaluation has been done to revise the PRA results. It includes

- installation of the 5rd EDG as a mitigation to station blackout;
- use of plant-specific fragility data for ESW Sluice gate and EChW/NChW hold down bolts;
- investigation of alternative connection arrangement for gas turbines;
- Replacement of 69 kV switchyard to GIS and housing G/T;
- ATWS procedure improvement;
- HPCS/RCIC suction changeover;
- installation of thermal-lag as fire safety separation;
- H_2 control system incorporation inside containment;
- emergency operating procedure improvement.

The total mean core melt frequency after implementing the betterment program is $9.6X10^{-5}$. This includes $5.3X10^{-5}$ from seismic, $1.0X10^{-5}$ from typhoon, $8.6X10^{-6}$ from ATWS, $3.9X10^{-6}$ from general transients, $1.8X10^{-5}$ from fires, $5.7X10^{-7}$ from floods, and $7.9X10^{-7}$ from LOCA.

A large fraction of dominant accident sequences are resulted from seismic external initiators. Two major categories are (1) loss of off-site power caused by seismic failure of ceramic insulators in the switchyard followed with the loss of high head core inventory makeup system (2) a large loss of coolant accident caused by seismically induced failure of recirculation pipes occurred with seismically induced station blackout. Different from that of Chinshan PRA, the important internal accident sequences have been resulted from ATWS instead of loss of off-site power. The two major scenarios are loss of feedwater with and without reactor isolation transients resulted ATWS followed with failure of early stage high head core inventory makeup. It is noteworthy that the CMF resulted from typhoon events is higher than that in Chinshan PRA. The main reason for this discrepancy comes from the difference in analytical method for achieving the hazard curves and the fragility data for the turbine building and gas turbine building.

II.3 - Maanshan PRA

The result of Maanshan PRA analysis exhibits a total CMF of $1.1X10^{-4}$ per reactor-year. The CMF for internal initiating events as a group, for the specific internal initiating events, and for seismic events, typhoons, fires, and flood are summarized in Table I & II.

The result shows that the internally initiated sequences (33%), seismically induced sequences (32%), and typhoon-induced sequences (24%) contribute approximately equally. Sequences resulting from fire contribute about 11% and flood less than 1% to the total CMF.

Therefore, the three dominant sequences are discussed (1) those arising from internal initiating events (2) those arising from earthquakes (3) those following typhoons. External initiators like seismic, typhoon, and fires have contributed a large fraction on the overall CMF. All the top five sequences have similar scenarios induced by seismic/typhoon resulted loss of offsite or on-site electric power. Among the important internally initiated accident sequences, there are

- LOCA followed by failure of low-head decay heat removal and recirculation systems;
- loss of MFW without reactor trip given moderator temperature coefficient higher than -8 pcm/°F;
- medium LOCA followed by failure of low-head safety recirculation;
- failure of primary cool-down and to replenish RWST given SGTR without successful isolation;
- failure of bleed-and-feed given loss of MFW transient without successful AFW cooling;
- failure of turbine-driven AFW given station blackout.

Based on the engineering insights, a betterment program for the Maanshan NPP was performed simultaneously. It includes

- NSCW system and pump anti-vibration improvement;
- CCW system and heat exchanger improvement;
- EChW system and heat exchanger upgrade;
- emergency operating procedure review and improvement;
- A.C. power reliability improvement such as installations of fifth emergency D/G and housing G/T;
- ATWS capability improvement - "AMSAC" for additional automatic turbine trip logic;
- fire protection improvement;
- turbine driven AFW pump room cooling improvement;
- D.C. battery racks seismic design enhancement;
- 4.16 kV switchgear room flooding protection improvement;
- installation of startup motor driven MFW pump.

III - PROSPECTIVE PRA APPLICATIONS

The application of PRA technology to the regulation of nuclear power station can be benefitted from two aspects. As an integral consideration, a base-line PRA estimate such as CMF, containment failure frequency, expected offsite consequences, etc. can be used as a rule to evaluate the design and safety level of a nuclear power plant. A high CMF can be an indication of a poor design/operation. Furthermore, by examining the sources of different contributions to the aggregate value, specific areas of design weakness can be pin-pointed. Typical application in this aspect includes

- to demonstrate that the likelihood of core damage will be less than 1.0E-05 per reactor-year in EPRI-ALWR goal (or described in SECY-90-16);
- the expected mean frequency of occurrence of offsite doses in excess of 25 rem beyond a half mile radius from the reactor is to be less than 1.0E-6 per reactor-year, considering both internal and external events;
- the containment design is to assure that its conditional failure probability is less than 0.1 when weighted over credible core damage sequences.

By contrast, differential calculus can be used to examine how a nuclear power plant's risk varies with time. It serves as a tool to evaluate the dynamic operation of a nuclear power plant. There are several mechanisms that can cause plant risks to change significantly over time such as degrading of individual components or whole systems due to poor maintenance and improvements due to proper design modification or enhanced maintenance. It is possible for the plant configurations to change from time to time as certain components are removed from (or restored to) service for tests and/or maintenance, while others may be removed through failure. The configurations also may change when going from one plant operating mode to another, such as going from power operation to shutdown. Since the risk significance of a component or system is also a function of the plant's configuration, a configuration change yields a corresponding risk level. A differential calculus application of PRA analyses can determine the changes in risk due to changes in component performance, availability, and plant configuration.

Differential calculus PRA analyses are often tied to relative risks. However, integral calculus PRA analyses are more associated with absolute risks. Therefore, differential PRA applications minimize decision-making concerns due to uncertainties in absolute "bottom line" risk values. The major potential applications in this aspect include

- establish specific procedures for determining Allowable Outage Times (AOTs) and Surveillance Test Intervals (STIs) both on a generic and plant-specific basis;
- evaluation of specific issues, identified following this method, that affect AOTs and STIs;
- procedures for evaluating case-by-case requests for (i) AOT extensions and (ii) STI extensions;
- identification of specific interfaces with reliability assurances and reliability monitoring activities and other research needs for Technical Specification optimization.

Another approach to utilize risk information of PRA results is to produce a risk-based inspection plan. With the given logic equation consisted of minimal cutsets that represent dominant failure paths leading to a top event (core meltdown), the importance of each significant basic event can be measured. In order to rank for a risk-based inspection plan, Fussell-Vesely importance shall be used since it considered both component reliability and the component safety significance. A guideline for allocation inspection resources can be determined after ranking the Fussell-Vesely importance for each basic event. In this part, equipment and/or plant operating procedures is reviewed to reflects their effectiveness in improving the identified basic event. This has resulted in some new inspection areas which have not been intentionally specified in conventional inspection program.

When compared to conventional inspection program, this methodology has the following advantages:

- This approach objectively determines inspection items through risk-based information; while in conventional way, inspection items are subjectively determined by engineering judgement;
- With the ranking procedure, the users can optimize inspection resources based on their specific purpose. The described safety-oriented inspection program have ranked the priorities according to Fussell-Vesely importance. For a safety-oriented inspection program, they may use risk achievement worth as a ranking index since people may consider safety with no consideration on cost.

As a typical application, accident sequences that are resulted from external initiating events and that involve containment analysis have not been included in our importance ranking. Furthermore, application should be extended to cover these categories of sequences.

The risk-based inspection plan can also be extended to cover some specific programs like the implementations of GL-89-10, "Safety-Related MOV Testing and Surveillance". The program requires licensees to be responsible for satisfying regulations if activities performed in response to GL-89-10 reveal that an MOV is not capable of performing its safety functions adequately. The program will take several years before completing the plant-wide MOV testing. Following the importance ranking, licensees or regulators can concentrate on some certain highly safety related MOVs instead of random choice. This can significantly upgrade plant safety even during ongoing of the program.

IV - CONCLUSIONS AND RECOMMENDATIONS

In order to better understand the significance of the various core melt sequences in the PRAs, there are a number of items which need to be further investigated. Beyond uncertainties in the input failure data, extra uncertainties exist in both the seismic and typhoon hazard analysis and in the plant response to an anticipated transient without scram. A number of these items and the importance of various assumptions concerning operator performance and plant equipment are discussed in the following paragraphs.

IV.1 - Seismic Analysis

There are two major areas for uncertainty to be generated in the seismic analysis; first the development of the hazard curve expressing the expected frequency of a given ground acceleration at the site and secondly the predicted acceleration at which a given component will fail. The plant is designed to withstand relatively high accelerations and the occurrence of earthquakes giving accelerations which have a high likelihood of damage are rare and therefore the predicted frequency is an extrapolation from lesser earthquakes. Similarly, the majority of the components are not tested at the higher acceleration values. The failure of the ceramic insulators in the switchyard is, however, postulated to occur with a moderate value of 0.3 g which is based on limited failures which have actually occurred in the United States. So there is a greater degree of confidence in the parameterization of this failure, which is the most important in the seismic analysis, than some of the others, for which much higher values are assigned, but which are less important. Sensitivity study has shown that the reduction in the uncertainty of critical fragility may drastically reduce the seismically induced CMF. (A 25% reduction in the uncertainty of fragility may result in the 90% upgrade in seismic induced risk.)

IV.2 - Human Error Probability

System or function failures can result from failure of the operator to perform certain functions or to perform the function incorrectly and consequently to result in component failure. Therefore, operator actions are included in both the event trees and fault trees. Human actions are usually formulated in the higher level of fault tree and hence may result in higher structural importance. There is, however, difficulties in quantifying human error probabilities due to the following characteristics:

- It is often difficult to determine factors that constitutes a human error;
- People don't err unless given the opportunity;
- People are especially prone to "common-mode" errors;
- People tend to discover their own errors and correct them;
- Errors in some industrial production operations may not be employed for nuclear power plants;
- There are hardly well-accepted theories for the quantification of human error rate.

Human reliability, although it may sound like, is not analogous to machine reliability. The method to quantify human error probability is still resorted to subjective expertise and some semi-empirical formulation.

IV.3 - Common Mode Failure

There are minimal cutsets that are the product of the failures of two or more similar components. However, the failures of the components are judged not to be necessarily independent, the value of the cutset must be modified to include the possibility of dependent failures. System analysts generally aim to model explicitly the major common cause mechanisms. They incorporate dependencies between failures, such as those that result from common support systems (e.g., component cooling water), explicitly in the fault tree for the system. Therefore, these dependencies cannot be included in the estimate of common mode failure probability, since this would lead to double counting. However, as mentioned previously, there are other possible causes of dependent failure - for example, manufacturing errors, errors due to a common maintenance act, and unusual environmental conditions. It is the residual common-cause failures that contribute to common mode failure probability, and the analyst must be careful to screen the data used to ensure that only the relevant contributors are used in estimating common mode failure probability.

In addition, there may be some other physical phenomena which contribute to the CMF. In many cases, public risk relies on experts' opinion to supplement the sparse database. Typical examples include reactor coolant pump seal LOCA model, credit for gas turbine generator, V sequence formulation, and some containment failure modes, etc. As the original safety goal has been originated from the definition "less than 0.1% increment in public risk", some of the expertise judgement should be equally applied to the other societal risks for comparison. From the regulation point of view, the PRAs have been based on compact formulation with conservative assumptions in data assessment. However, from the consistency viewpoint, a great fraction of risk have been resulted from the knowledge uncertainty, for example, in the external event contributions such as like seismic and typhoon analyses. The comparison for 0.1% risk increment shall include the expansion of other industrial risks resulted from the same subjective judgmental data.

Experiences has increased its significance in recognition of the usefulness of PRA methodology to evaluate plant risk for the total spectrum of potential accident sequences. The majority of the methods used in the studies are described in the PRA procedure Guide (USNRC, 1983) and also in EPRI-ALWR document. However, some techniques used in the analysis of the externally initiated events, the human factors analysis and the impact of accident on the containment represents the state of the art in these areas. The applications of PRA are broad and useful in many current undergoing programs and also in areas of design process.

REFERENCE

1. HERCHEL SPECTER, "*Risk-Based Regulation,*" ANS meeting, Boston, MA, USA, June 1992.

2. Y.C. YEH, C.F. CHUNG, and D.Y. HSIA, "*Development of a Risk-based Inspection Program,*" Proceedings of the Sixth Sino-Japanese Symposium on Nuclear Safety, Tokyo, Japan, Dec. 1991.

3. "*Final Report- Probabilistic Risk Assessment of Chinshan Nuclear Power Plant,*" Atomic Energy Council, Taipei, Taiwan, Republic of China, 1991.

4. "*Final Report- Probabilistic Risk Assessment of Maanshan Nuclear Power Plant,*" Atomic Energy Council, Taipei, Taiwan, Republic of China, 1987.

5. "*Betterment Program Following KS PRA: Rev. 1,*" Taipower Company, Taipei, Taiwan, Republic of China, 1988.

6. "*Final Report- Probabilistic Risk Assessment of Kuosheng Nuclear Power Plant,*" Atomic Energy Council, Taipei, Taiwan, Republic of China, 1985.

7. W.E. VESELY, "*Procedures for Evaluating Technical Specifications: Evaluation of Allowed Outage Times from a Risk and Reliability Standpoint,*" Battelle Columbus Laboratories, Columbus OH, USA, June 1985.

8. "*PRA Procedure Guide - A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants,*" NUREG/CR-2300, USNRC, 1983, Washington D.C.

Session 20
Application of PRA/PSA in Design and Modification-II

Session 20
Application of PRA/PSA in Design and Modification-II