GT-2700134

UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, D.C. 20555-0001

August 14, 2001

MEMORANDUM TO: ACRS Members

FROM: Michael T. Markley, Senior Staff Engineer

SUBJECT: NUCLEAR ENERGY INSTITUTE LETTER CONCERNING THE ELECTRIC POWER RESEARCH INSTITUTE PAPER ENTITLED, "SAFETY BENEFITS OF RISK ASSESSMENT AT U.S. NUCLEAR POWER PLANTS"

The purpose of this memorandum is to forward the Nuclear Energy Institute (NEI) letter concerning the Electric Power Research Institute (EPRI) paper entitled, "Safety Benefits of Risk Assessment at U.S. Nuclear Power Plants" for consideration by the Committee.

Background

On June 28, 2001, NEI forwarded the EPRI paper to Chairman Meserve encouraging the NRC to communicate to all stakeholders how PRA has been developed and used, and to provide a context for ongoing NRC and industry efforts. The paper appears to promote the notion that improved industry performance has a direct linkage to the use of risk information. It compares nuclear risks with societal risks, highlights risk trends using average core damage frequency and illustrates risk reduction over time, and uses plant measures such as scram reduction rate and capacity factor performance to suggest that the "risk level" has a proportional relationship to certain performance indicators. While encouraging the NRC to communicate to stakeholders on this matter, the ongoing stakeholder concern of making the plant-specific results of probabilistic risk assessments (PRAs) publicly available does not appear to be well addressed in the NEI/EPRI documents.

The NRC staff plans to provide a written response to the NEI request. In preparing its preliminary response, the staff inquired whether the ACRS was interested in responding to NEI on this matter. The staff made this request, in part, based on past ACRS report to Chairman Meserve on the Union of Concerned Scientists report entitled, Nuclear Plant Risk Studies: Failing the Grade."

The ACRS staff forwarded the NEI/EPRI documents to Dr. Apostolakis for consideration. Dr. Apostolakis does not see the need for the Committee to formally comment on the EPRI report and recommends that this item not be added to the ACRS future activities list. Therefore, it is being provided to the Committee for their information only.

Expected Committee Action

No Committee action is expected at this time.

Attachments: As Stated
cc w/o attach: ACRS Staff and Fellows

ML011900152

NUCLEAR ENERGY INSTITUTE

Ralph E. Beedle
SENIOR VICE PRESIDENT AND
CHIEF NUCLEAR OFFICER,
NUCLEAR GENERATION

June 28, 2001

The Honorable Richard A. Meserve
Chairman
U.S. Nuclear Regulatory Commission
Mail Stop O-16 C1
Washington, DC 20555-0001

Dear Chairman Meserve:

The nuclear industry and the NRC have used probabilistic risk assessment (PRA) technology extensively over the last two decades to improve nuclear plant safety. These past efforts provide a solid foundation for the risk-informed initiatives under development today both within the industry and the NRC. We believe it is important for the NRC to communicate to all stakeholders how PRA has been developed and used, and to provide a context for our ongoing efforts.

The enclosed paper entitled *Safety Benefits of Risk Assessment at U.S. Nuclear Power Plants* was developed by EPRI at the request of NEI's Risk-Informed Regulation Working Group. It provides a history of the development of PRA, compares the relative risk of nuclear plant operation with other societal risks, presents a sampling of the applications of PRA by both the industry and NRC, and discusses how a risk-informed safety culture has emerged to enable a new era of safe, cost-effective operations.

We look forward to future interactions with the NRC on the continued development of risk-informed regulatory initiatives. We trust that the paper will aid in providing a common understanding and context for these initiatives.

Sincerely,

Ralph E. Beedle

Enclosure

c: The Honorable Greta Joy Dicus
The Honorable Nils J. Diaz
The Honorable Edward McGaffigan, Jr.
The Honorable Jeffrey A. Merrifield
Dr. William D. Travers
Mr. Samuel J. Collins
Mr. Ashok C. Thadani

1776 I STREET, NW SUITE 400 WASHINGTON, DC 20006-3708 PHONE 202.739.8088 FAX 202.785.1898

SAFETY BENEFITS OF RISK ASSESSMENT AT U.S. NUCLEAR POWER PLANTS

John Gaertner
EPRI

Doug True
ERIN Engineering and Research, Inc.

June 2001

SUMMARY

- **U.S. nuclear power plants have improved safety and have evolved to a risk-informed safety culture through application of Probabilistic Risk Assessment (PRA). Nuclear plant PRA has matured from 1975 to today: every plant has models, expertise, and PRA application experience.**

- **Risk to the public from U.S. nuclear power is very low relative to NRC safety goal policy and relative to other risks. Calculated risk has decreased threefold in the past decade, while trends of indicators such as plant scram rate, capacity factor, and safety challenges show marked improvement.**

- **Insights from PRAs have established which initiators, equipment, and human actions are risk-important and have helped to foster a new plant culture of risk management. Many detailed examples illustrate the scope and magnitude of changes that either reduce risk or simplify plant operations while maintaining a low level of risk. Some of these changes were enabled by risk-informed regulations, petitioned by owner/operators or initiated by NRC.**

- **The above observations establish that the industry is positioned for more risk-informed improvements. Continuing change in regulations and attitudes about risk-informed and performance-based operations is necessary.**

1. INTRODUCTION

Probabilistic risk assessment (PRA) and safety risk management are commonplace tools in today's U.S. nuclear power plant. Risk assessment provides insights on the importance of equipment, human actions, and safety challenges with respect to public safety. Numerous safety improvements have been implemented as a result, and a new risk-informed safety culture has emerged.

This paper describes the evolution from a deterministic compliance culture to a risk-informed safety culture. It presents data and case studies that illustrate the benefits of this change. It challenges stakeholders to understand and exploit the power of risk-informed decision making to enable a new era of safe and cost-effective plant operations.

2. BACKGROUND

The safety design and regulation of U.S. nuclear power plants have traditionally been based on deterministic and prescriptive criteria and requirements. These criteria and requirements employ numerous conservative conventions to ensure safety such as design basis accidents, defense-in-depth, single failure criteria, and margins of safety. At the time these requirements were set, conservative criteria were justified because of the lack of experience with nuclear power.

The first large-scale risk assessment of a nuclear plant was the Nuclear Regulatory Commission (NRC) Reactor Safety Study (WASH-1400) in 1975. It quantified the risk of two nuclear power plants in terms of reactor core damage frequency (CDF), radioactive release frequency, and public health impacts. Furthermore, it prioritized the contributors to risk in terms of initiators, equipment, mitigation functions, and human actions.

Several utility PRAs emerged in the early 1980s. Among these, the Big Rock Point PRA and the Oyster Creek PRA were performed to prioritize and justify safety changes. The Zion, Indian Point 2, and Limerick PRAs were performed by utilities to characterize risk to large nearby populations. The Oconee PRA was performed by EPRI and utilities to demonstrate PRA methods, train practitioners for utilities, and provide a model for future utility studies. More PRAs followed. Meanwhile, NRC conducted comprehensive PRA studies of five plants with diverse designs and published the results as NUREG-1150.

In 1988, NRC requested all plant licensees to complete Individual Plant Examinations (IPEs) to verify plant safety and to identify accident vulnerabilities. In response, 74 PRAs, representing 106 U.S. nuclear plants, were created using CDF and Large Early Release Frequency (LERF) as figures-of-merit for risk. Since 1992, when these studies were completed, owner/operators have maintained their PRA models, used them for numerous risk-informed decisions, and have enhanced their PRA capabilities. The result has been 1) a new understanding of safety contributors and priorities; 2) a demonstrated ability to improve safety while improving availability, reliability and cost-effectiveness; and 3) an opportunity to simplify plant regulation from deterministic to risk-informed and from prescriptive to performance-based.

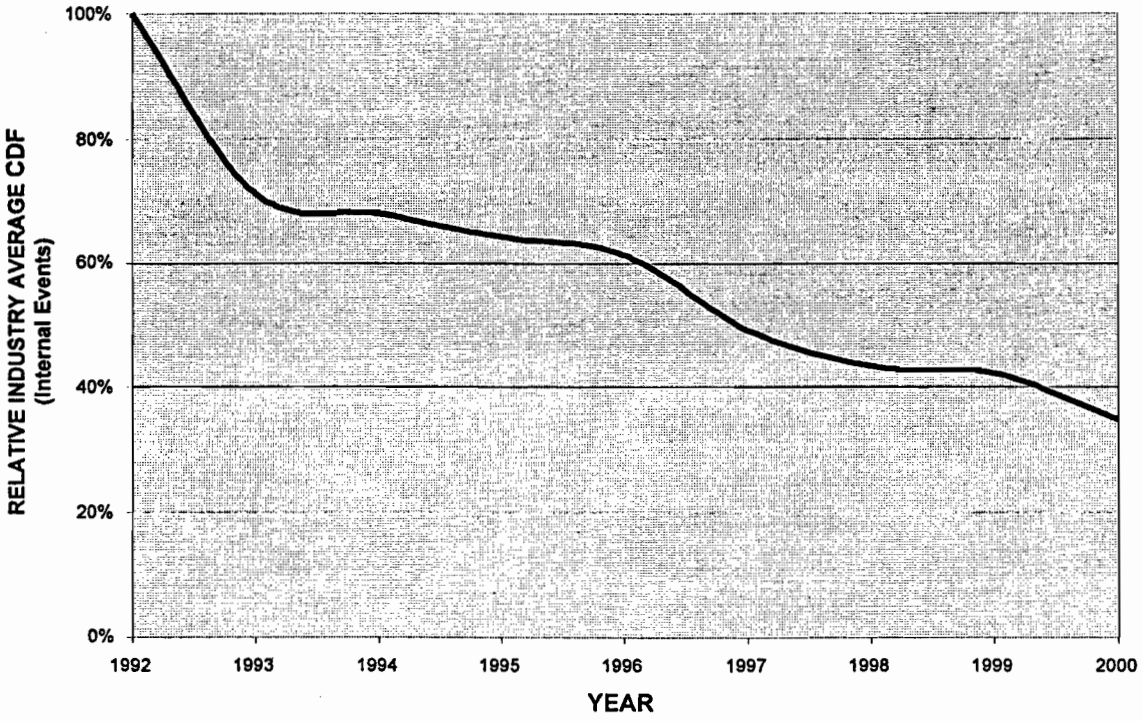
The remainder of this paper presents data and case studies to illustrate these changes.

3. QUANTITATIVE IMPROVEMENT IN PERFORMANCE SINCE PRA

3.1 Industry Risk Trends

The IPEs provide estimates of CDF for each operating nuclear unit. A primary purpose of these examinations was to provide a plant specific estimate of the relative likelihood of various core damage contributors. The results in 1992 verified U.S. nuclear plant safety. Nonetheless, nuclear power plant owner/operators identified cost effective means to address vulnerabilities and reduce the overall likelihood of a severe accident. Since the IPEs were completed, there has been a significant downward trend in calculated risk levels due to plant improvements and better understanding of risk contributors. The industry average CDF from internally initiated events dropped by nearly a factor of three from 1992 to 2000. Figure 3-1 provides a year by year estimate of the industry mean CDF based on a compilation of plant-specific PRA results.

Figure 3-1
Trend in Industry Average Core Damage Frequency



The initial period following the completion of the IPEs is marked by a sharp decrease in average CDF as plants modified their design or practices to reduce risk from identified challenges. Two of the largest calculated risk reductions identified in plant IPEs involved a) beyond design basis floods with the potential to damage both trains of safety systems, and b) provision of alternate cooling capability for a key safety system. From 1993 to 1995 the industry focused on the assessment of risks from earthquakes and fires as part of the IPE External Events (IPEEE) analyses. Also during that time, the initial industry efforts were undertaken to develop methods for utilizing PRAs in the decision-making process. One key milestone in this process was the issuance of the EPRI PRA Applications Guide. This document provided the first comprehensive framework for evaluating the risk significance of plant changes and provided an impetus for the NRC's efforts to develop risk-informed methods for regulatory decision-making. From 1996 to present, the calculated industry average CDF has continued to drop as a result of industry safety management activities. Section 5 provides a number of specific examples of risk reduction measures undertaken by owner/operators.

The other significant risk metric evaluated in current risk-informed applications is large early release frequency (LERF). PRAs show that large radioactive release cannot occur unless there is prior core damage, and most core damage events are contained in the plant without a large release. Therefore, industry average LERF is low. It is difficult to obtain a trend graph of LERF since it was not directly reported in the IPE, but it is generally agreed that the trend is either steady or decreasing.

3.2 Comparative Public Safety Risk of Nuclear Power

Nuclear plant owner/operators typically use CDF and LERF as figures-of-merit to represent their risk profile. The NRC considers these figures-of-merit to be surrogates for their Safety Goal measures of public risk; that is, individual early health effects and individual latent health effects, respectively. Several industry and NRC studies have estimated nuclear power risk relative to Safety Goals as well as the surrogate figures-of-merit. Furthermore, we can compare these estimated risks to measured risks from

other causes. It is important to note that all values in this table are based on actual mortality statistics except for the nuclear plant accident entries. These are calculated values -- there has never been measurable harm to any individual in the public from a U.S. nuclear plant accident.

Figure 3-2 below provides a comparison of nuclear power mortality risk with other risks and with the NRC Quantitative Health Objectives (QHO) derived from their Safety Goals. The QHOs are estimated by taking 0.1% of the "all accident" rate and the "cancer" rate respectively. The ranges for nuclear power risk are based on risk results from NUREG-1150, so they do not reflect improvements made since 1992. They reflect variations from plant to plant and have been increased, using engineering judgment, to account for additional accidents that may not be calculated in the PRA model.

Figure 3-2
Comparison of Mortality Risks for U.S. Population

Cause	Deaths per 100,000 per year	% from this cause
All Causes	920	100
Cancer	220	24
All Accidents	35	4
Motor Vehicles	17	2
Fires	1.5	.002
Natural Disasters/Weather	0.7	.0008
Air Travel	0.3	.0003
Nuclear Plant Accident early health effect[1]	0.000004 to 0.004	<.000004
Nuclear Plant Accident latent health effect[2]	0.00004 to 0.004	<.000004

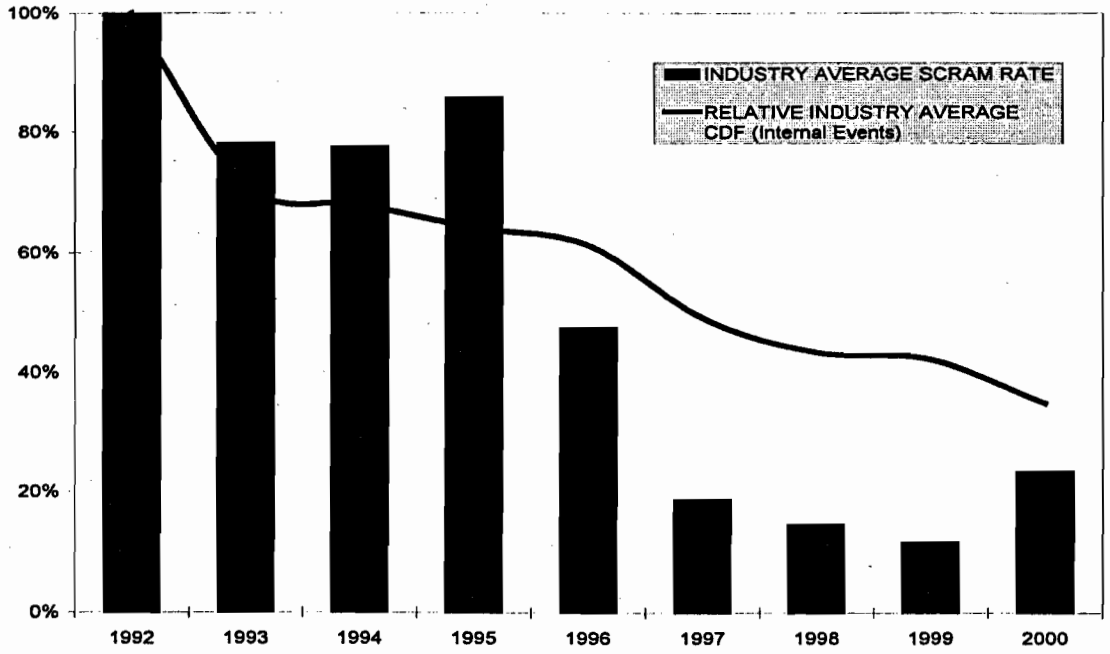
[1] Only if within 1 mile of a plant. Varies by plant. NRC QHO is 0.035 deaths per 100,000 per year.
[2] Only if within 10 miles of a plant. Varies by plant. NRC QHO is 0.22 deaths per 100,000 per year.

The figure clearly shows that U.S. nuclear plants contribute very low risk relative to NRC safety goal policy and relative to other risks to the public.

3.3 Plant Risk and Plant Performance

Over the past decade, the U.S. nuclear power industry has seen extraordinary improvement in plant performance. Some have questioned whether the industry's efforts to improve plant performance may have reduced safety. In fact, the opposite is true. The industry has seen risk levels drop while most economic performance indicators have shown significant improvement. For example, one principal measure of plant performance is the number of plant scrams, or reactor trips, per year. Figure 3-3 provides a comparison of the industry average risk levels versus the industry average scram frequency. This figure shows that the scram rate has dropped simultaneously with the drop in CDF. Overall, the industry average scram rate per year has dropped by more than a factor of four over the time period 1992 to 2000.

Figure 3-3
Scram Rate Reduction vs. Risk Levels



Plant scram rate is one indicator of plant performance, but a stronger indicator of the ability of a plant to meet the production needs of its customers is capacity factor. In simple terms, capacity factor measures the relative production of a facility against the total possible production which could have been achieved if the plant had been producing power at all times.

Figure 3-4
Capacity Factor Performance vs. Risk Levels

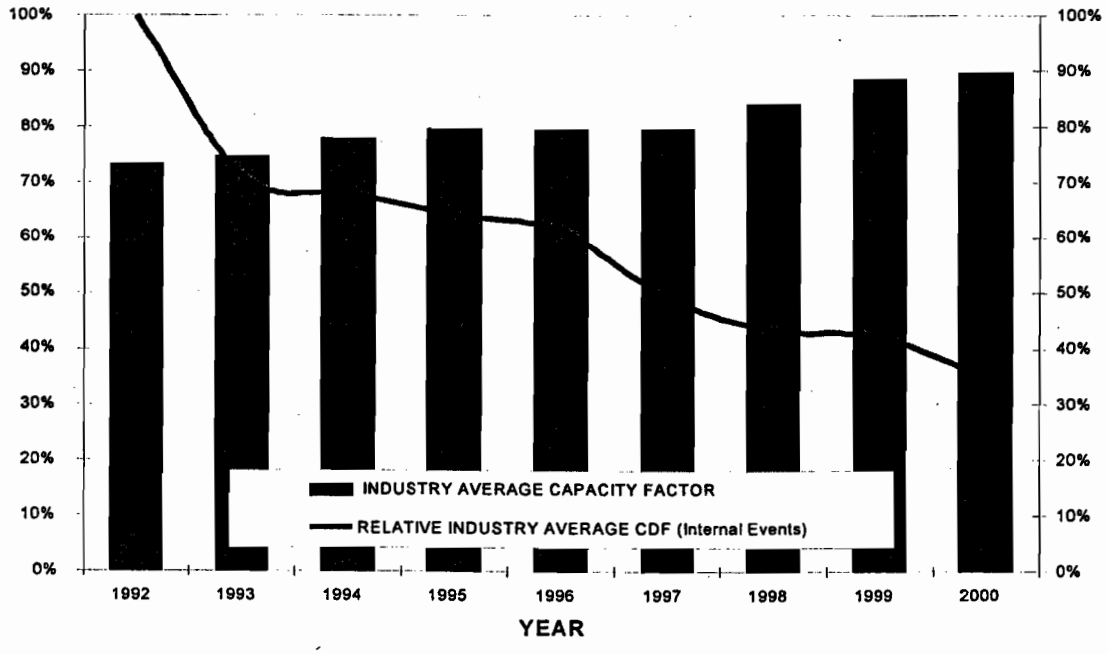
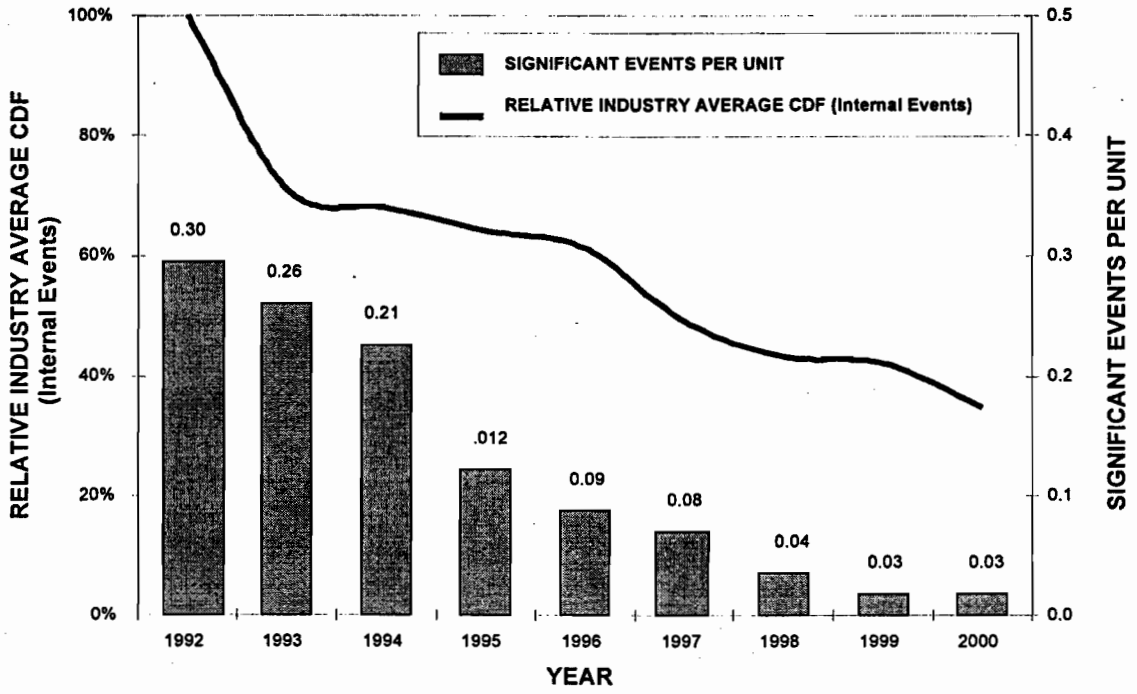


Figure 3-4 provides a comparison of industry average capacity factor over the same timeframe. Here again, the improvements in capacity factor performance occurred over the same time period when plants were reducing risk. Finally, we would expect the trend in risk reduction to be accompanied by a favorable trend in the number of safety challenges. This is in fact the case. Figure 3-5 displays the annual average number of "significant events" reported as required to the NRC. The figure shows a tenfold reduction in unit event frequency over the time period when plants were reducing risk.

Figure 3-5
Number of Safety Challenges vs. Risk Level



4. BRIEF DESCRIPTION OF THE PRA ANALYSIS PROCESS

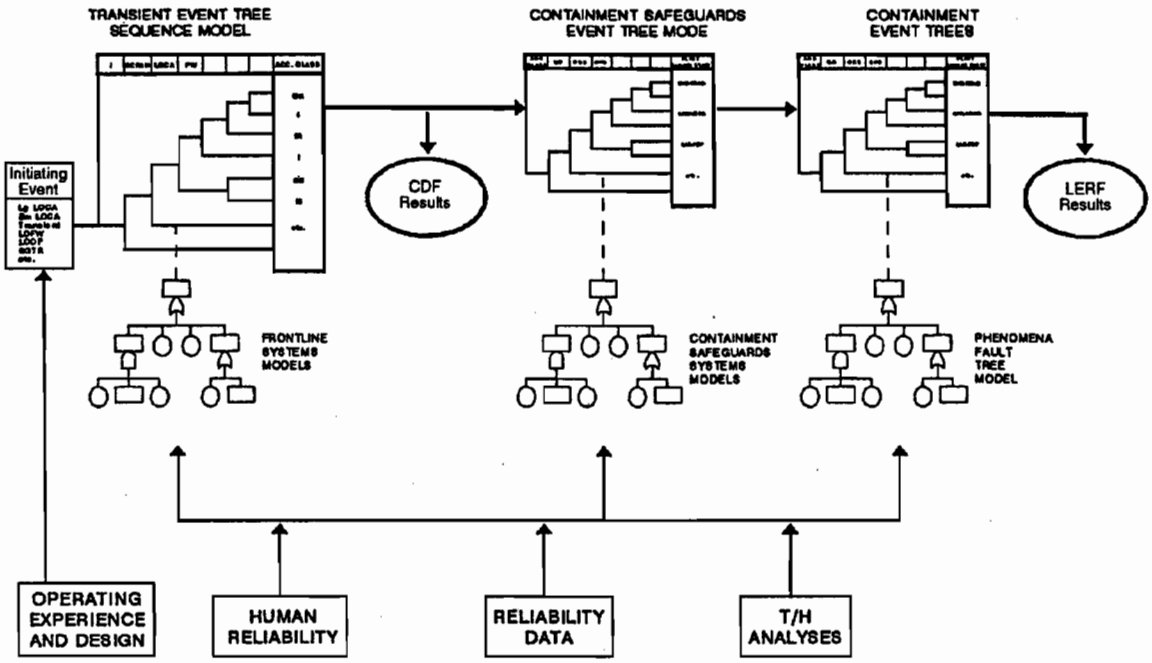
PRA studies start by identifying all potential events that could lead to an accident. This could include the rupture of a pipe, a failure of an electrical system, or any other potential "initiating events". Data on plant performance has been compiled from the many years of plant operation. Using this data, the likelihood of these initiating events is calculated. Even events that could be expected to occur only once in a million operating years are included. For rare events the probability of occurrence is estimated through established statistical and engineering techniques.

The next step in the assessment is the construction of a unique computer model of each nuclear plant. The overall model is a complex mathematical representation of logic models; e.g., linked event trees and fault trees as shown schematically in Figure 4-1. Elements of the event trees are important system and human response to initiators and subsequent plant conditions. Elements of the fault trees are individual equipment and human failure probabilities. Models employ detailed design information, operating procedures, thermal-hydraulic modeling, human error modeling, operating experience analysis, and equipment performance data analysis.

The first part of the model, PRA Level 1, uses the initiators as seed events to identify the sequences of events and to calculate the frequency of failure sequences which result in core damage. The second part of the model, PRA Level 2, uses core damage sequences as seeds to produce all of the sequences of further failures and events in the containment which result in radioactivity release. The containment is the structure and its systems that prevent release to the environment. The typical figure-of-merit is LERF.

Most nuclear plant PRA studies end at Level 2, but analysis can continue to Level 3, identification of sequences leading to public health effects and their frequencies. Early health effects and latent health effects are commonly analyzed to compare with the NRC safety goals and QHOs. Figure 4-1 is a schematic representation of the nuclear plant PRA process through Level 2.

Figure 4-1
Nuclear Plant PRA Analysis Process



5. INSIGHTS FROM EARLY PRA APPLICATIONS

5.1 Generic PRA Insights

The early applications of PRA to U.S. nuclear plants resulted in a gradual change in the safety culture of the plant staffs. This change resulted from the following important insights:

1. **Design basis accidents and other anticipated accident initiators at the time of plant design did not pose the highest risk to public safety.** Large loss-of-coolant-accident (LOCA), steam line breaks, and feedwater line breaks are examples of such initiators. The design of the plants and the development of operator procedures and training to respond to these initiators was shown to be very effective, and no additional emphasis on these accidents has been necessary based on the PRA results.
2. **More common initiators such as automatic plant trips, loss-of-offsite power, and small LOCAs posed the highest risk among internal event initiators.** This risk was partly the result of the relatively high frequency of these challenges. However, much of the risk was caused by failures to successfully achieve all the functions necessary to mitigate the accidents. Owner/operators have responded by dramatically reducing the frequency of plant trips, improving the response to loss-of-offsite power, and greatly reducing the chances of inducing a small LOCA during a transient response.
3. **Risk from dominant contributors was often plant-specific and was easily reduced by relatively inexpensive design changes or procedure changes.** This fact enabled owner/operators to achieve significant safety improvements immediately, and it demonstrated the value of plant-specific PRA analysis.
4. **Only a fraction of safety equipment is truly important to the prevention or mitigation of events which contribute most to plant risk.** Because the PRA employs an integrated, objective model of

the plant to the component failure-mode level, it is able to measure the importance of each piece of equipment to the total risk. One study reports that "50 to 500 active components control/determine about 90% of the CDF." The important insight here is to ensure that these critical components receive adequate attention and that resources are not inappropriately diverted to less risk-important equipment.

5.2 Plant Specific PRA Insights

This section provides a number of specific examples of risk reductions achieved by owner/operators as a result of PRA analyses. In nearly all cases, the scenarios which indicated that plant safety could be improved were outside the original design basis of the plant and the changes were voluntarily implemented by the owner/operator.

Reliability of Reactor Coolant Pump Seals

Risk assessments have highlighted the importance of reactor coolant pumps in pressurized water reactors (PWRs) during a plant transient. Reactor coolant pumps simply circulate the water through the reactor during normal operation. Their operation is not necessary for safe shutdown. However, they have complicated seals that must be kept cool and at the proper pressure using a water injection system until the reactor vessel is depressurized. Otherwise the seals will leak, creating a small LOCA during plant shutdown. This LOCA creates another challenge to shutdown, and increases the chances of the initiator leading to an accident.

In response, owner/operators have made various plant improvements. Each plant has a unique solution based on its vulnerability and design. PRA accident sequences show the importance of operator action to stop the reactor coolant pumps if necessary, to align alternative injection to the seals, or to provide alternative power to the seal injection system. PRAs identified the times available to operators for their actions, and they identified the plant conditions and equipment configurations that would exist in each important scenario. With these new insights, procedures were changed to carefully operate and monitor the pumps and their support systems. Some plants have provided diverse injection options from other systems which require no station power (loss of all station power was found to be likely cause of the problem). One plant PRA identified a subtle dependency whereby a single injection train would require both emergency power busses during a loss of offsite power. This dependency was subsequently removed by a design change. After careful review of options, one plant elected to change its seals to another style, which is more rugged. This plant reduced total CDF by 30% from the seal change alone.

System Cross-ties

One of the strengths of PRA is the ability to evaluate system interactions and dependencies. Many plants have found that providing additional capabilities to cross tie and back up systems can be beneficial, particularly for systems like electric power and cooling systems. These systems are often referred to as "support systems" because their function is to support the "front-line" systems, such as emergency core cooling systems, which directly mitigate accidents.

One example of such a capability comes from a Westinghouse PWR. In this plant, the safety related service water systems perform a number of key functions, including cooling of emergency core cooling systems and reactor coolant pump seals. As discussed above, left without cooling, the reactor coolant pump seals can leak. Loss of service water can lead to both loss of seal cooling and loss of core cooling. One two unit plant site identified that the use of a cross-connection between the units service water systems could provide additional protection in the event service water cooling was lost at one unit. Crediting this cross-connection capability resulted in a 25% reduction in the CDF for each unit.

Electrical systems also play an important role in reducing risk. Some plants, particularly multi-unit sites, have the capability to crosstie AC and/or DC power supplies to back up the loss of the primary supply. In one case, the provision of a crosstie capability between the 4kV electrical safety buses at two units resulted in a 35% reduction in CDF. In addition, the same plant found that supplying a small generator onsite could provide a backup to some essential plant instrumentation power supplies. This change resulted in an additional 66% reduction in CDF for a total reduction of nearly a factor of five.

Internal Plant Flooding

One very substantial risk improvement from PRA was the reduction in CDF from internal plant flooding. At one plant, the PRA modeled a scenario initiated by the rupture of a large condenser-circulating water pipe carrying non-radioactive cooling water to the turbine building basement from a lake upstream of the plant and at a higher elevation. Upon rupture of the pipe, numerous operator actions both inside and outside the control room would be required to reduce the flow rate into the turbine building basement. Even then, unisolated flowpaths could sustain the flow up to 100,000 gallons per minute, many times higher than the capacity to drain the water. As a result, equipment in the basement would be submerged, and would directly or indirectly fail emergency feedwater pumps, service water pumps, high and low pressure reactor core cooling pumps, reactor building spray pumps, and other equipment that could be used for achieving safe plant shutdown in this event. One important non-safety system, compressed air, was affected. Air was required to close valves to reduce the flow of the floodwaters. Sufficient equipment remained to bring the plant to a safe shutdown, but the CDF contribution of this scenario was unacceptably high and dominated all other risks.

The owner/operator took significant actions to reduce this risk. Penetrations were sealed up to a height of 20 feet, watertight doors were strengthened, and drains were redesigned. Level alarms were installed to give early warning to operators. Valve alignments were changed to limit water flow, valves which required compressed air were closed, and switches were added in the control room for control of other critical valves. Emergency operating procedures were rewritten to cope with this event based on the specific PRA scenarios. Backup systems were provided to improve the reliability of core cooling and reactor system integrity, both of which would be degraded by the flood.

The modifications made to the plant as a result of the PRA insights reduced the CDF contribution from internal flooding by a factor of about 60, and the total CDF was reduced by a factor of about 30.

BWR Containment Venting

The NRC's initial risk assessment, WASH-1400, identified that long-term decay heat removal was a risk significant function at boiling water reactors (BWRs). Normally, the main condenser provides the heat removal path. Under accident conditions when the main condenser is not available, the residual heat removal system (RHR) is used. Numerous PRAs have identified a significant benefit from providing an additional means for containment heat removal: containment venting. Containment venting involves opening a vent pathway from the containment to allow the steam generated by the cooldown of the reactor to be released. This controlled venting prevents the containment structure from being challenged by the long-term build up of steam. BWR emergency operating procedures now include specific actions to utilize containment vents to control containment pressure. As a result, all BWRs have some method of venting containment to remove decay heat. One BWR investigated the risk increase associated with removal of the containment vent capability at their plant and determined that it could result in a factor of five increase in CDF.

Seismic Plant Response

This section illustrates that nuclear plant risk assessment addresses external hazards – such as fires, earthquakes, and tornadoes – as well as initiators which originate within the plant. As part of the IPEEE process, utilities were requested to evaluate the seismic susceptibility of their plants. This request did not require a quantitative PRA evaluation of seismic risks, and many plants performed a qualitative seismic analysis called a seismic margins assessment (SMA). This approach builds upon the insights gleaned from past seismic PRAs and allows key risk vulnerabilities to be identified. About half the plants, however, did perform seismic PRAs.

The risk analysis enabled the owner/operator to focus efforts on potential failures that are likely and consequential to public safety. At most plants, risk reduction was achieved as a result of SMA or seismic PRA. Changes included improved anchoring of critical equipment or heavy items which could fall on

critical equipment, spacing of electrical cabinets and battery racks to prevent interaction, replacement of critical relays which can lose contact or "chatter", monitoring or repairing corrosion of supports, and securing heavy loose equipment such as cranes.

Shutdown Risk Reduction

Increased attention to shutdown risk occurred in the early 1990s because of several occurrences of inadvertent reactor coolant drain-down or loss of heat removal from the reactor coolant during refueling outages. Exposure of fuel by drain-down or boil-down could be significant if safety systems are in maintenance and especially if the containment is not available. Owner/operators were motivated to ensure safety, but they could not afford unnecessary conservatism that would extend the length of refueling outages. PRA models and risk assessment methods provided tools to manage risk.

Shutdown risk assessment is very different from at-power risk assessment. Unlike at-power conditions, average CDF is not the singularly useful figure-of-merit. Reactor coolant boiling and core damage are figures-of-merit. Also, risk varies greatly within an outage and between outages at a single plant, so some plants use instantaneous core damage probability (CDP), and outage profiles of CDP are plotted for planned outages and as outages progress. Corresponding values of boiling are used. Because these models are run continually with constantly changing information, they are necessarily simpler. These models are well suited for work planning and for monitoring undesirable risk changes.

One of the first plants to create a shutdown risk assessment was a BWR. Before applying the model to future outages, they applied the model retrospectively to a previous outage. They identified several practices, which were changed for future outages to reduce risk.

For one, they changed a practice of early draindown of the suppression pool for inspection and repairs. Under the old practice, the risk assessment identified a high-risk period just before and just after fuel movement. Due to low total water inventory, vulnerability to inadvertent draindown was increased. Delaying the suppression pool draindown until after the upper pool was flooded for refueling, risk was reduced. Another change involved the practice of frequently swapping residual heat removal systems and trains to make fuel loading easier. The high risk of losing cooling during each train swap, once identified, was eliminated. The model also identified certain higher risk evolutions, which, although they could not practically be avoided, they could be carefully monitored and managed, once identified.

Failure Rates for Key Equipment

Nuclear plant owner/operators are achieving reduced safety risk by lowering failure rates of risk-significant equipment. The risk significance of this equipment is identified and quantified by PRA; the reduction in risk is quantified by comparing the accident frequencies using failure rates in the PRA before and after the improvement. This improvement is being accomplished by more effective condition-based monitoring and better preventive maintenance; that is, by increasing the attention to the most risk-significant equipment at the plant. The following examples illustrate this contribution at one large PWR.

Service water pumps continuously remove heat from the plant to the ocean during normal operation. During an accident, these pumps remove the decay heat to bring the plant to a safe, stable state. Even more important at this plant, the PRA identified that loss of all service water pumps from a common cause during normal operation would not only trip the plant, but the plant would have a degraded ability to remove decay heat and bring the plant to a safe, stable state.

Between the time of the original IPE and the present, the best estimate of the likelihood of a single pump to fail its safety mission has improved by a factor of 6. Because the PRA method gradually updates the old performance data with the new data as experience accrues, the PRA pump reliability has improved by a factor of three. The impact of these performance improvements is a nearly 50% decrease in CDF at the plant.

Emergency diesel generators stand by to power safety equipment in case both power from the plant generator and off-site power from the grid are lost. During an accident, these diesel generators start

automatically within seconds. Between the time of the original IPE and the present, the likelihood of a single diesel generator to fail to start has improved by a factor of 20, and the PRA diesel generator reliability has improved by a factor of five. The impact of this performance improvement is a nearly 35% decrease in CDF at the plant

5.3 Voluntary Risk-informed PRA Regulatory Applications

Risk-informed Technical Specifications

A number of utilities have pursued risk-informed operational improvements by evaluating the plant Technical Specifications, which set requirements for equipment testing, operability, and operating limits. While these changes were triggered by the desire to improve operational efficiency and reduce costs, a number have resulted in net risk reductions or reliability improvements. During the early 1990s many plants requested changes to the testing requirements for reactor protection systems. These changes provided justification for extension of test intervals for various protective devices, in part based on reductions in plant trip frequencies due to test-caused plant trips. Since plant trips are potential initiating events, these test interval extensions effectively reduced risk, while reducing operating costs.

More recently, a number of plants have pursued extension of emergency diesel generator (EDG) allowed out-of-service times. These extensions allow the performance of maintenance during plant operation that had previously required plant shutdown. This change allows utilities to improve plant availability and improve the quality of maintenance performed. PRAs verified that the risk impact of the longer out-of-service time is acceptable, while improvements in diesel reliability and outage risk are anticipated.

Finally, as part of the risk-informed Technical Specification activities, plants have identified compensatory measures that can result in significant reductions in risk, even though additional equipment is taken out of service. These compensatory measures involve the identification of appropriate administrative controls during key equipment maintenance and the re-scheduling of other equipment maintenance which could result in additional risk increases. One plant has found that while more maintenance can be done during power operations, careful scheduling of maintenance activities can result in a net reduction in plant risk. Such insights would not be possible without a PRA model to assist in the evaluation of configuration risks.

Risk-informed In-service Inspection

Nuclear plants contain many segments of important piping. As piping ages, it becomes more likely to crack, leak, and rupture from a number of aging mechanisms. Periodic piping inspections are costly and expose workers to radiation.

The industry has developed risk-informed in-service inspection programs, approved by NRC, that prioritize and reduce inspections with effectively no increase in risk. The process reviews piping for risk-critical segments using the PRA. The risk impact of ruptures in critical piping such as reactor coolant lines, feedwater lines, and main steam lines that can initiate accident sequences have been thoroughly studied by the PRA. For these segments, the initiator frequency is characterized based on the presence of a degradation mechanism, vulnerability to that mechanism, and condition of the piping. In this way, the inspection program is greatly reduced, and resources are dedicated to the most risk-significant piping.

About 80 percent of U.S. nuclear units are committed to implement risk-informed in-service inspection.

Risk-informed Valve Testing Prioritization

Some motor-operated valves (MOVs) are required to open or close under extreme pressure and flow conditions during an accident response. These conditions cannot often be duplicated in tests. Conservative analysis and extrapolation of test results is necessary to demonstrate the required capability with adequate margin. An NRC generic letter, GL89-10, requested plant owner/operators to develop and document an effective program for all such valves.

A number of plants chose to rank the candidate valves according to their risk contributions using a calculation capability of PRA software to develop quantitative measures of importance. High importance valves received the first baseline analysis and tests. They also were assigned the shortest interval for periodic testing. The PRA also indicated whether other valves, not previously identified by the program, must be added. In this way, the risk benefits were optimized relative to resources and schedule.

Some owner/operators have used the same risk-ranking method for air-operated valves with the same success.

Risk-informed Containment Testing

Prior to 1995, containment leakage testing requirements were deterministically set and were prescriptive. These tests were costly and exposed workers to radiation, yet PRAs consistently showed that public risk was insensitive to leakage rates 100 to 200 times larger than the prescriptive limits. Changing the allowed leakage rates was considered, but it would not have solved the above problems. Instead, NRC and the industry established a risk-informed, performance-based approach, 10CFR50 Appendix J Option B.

Under this option, integrated leakage testing intervals can be extended from less than two years to ten years upon completion of consecutive successful tests at a shorter interval. Test intervals for penetrations and valve trains can be extended from the refueling interval up to five years, again conditional upon successful test results. In every case, the risk increase from this change was shown to be always less than one percent.

Most U.S. nuclear units now use this risk-informed testing option.

Configuration Risk Management

Plant-specific PRAs provide a unique tool for the assessment and management of plant configuration; that is, what equipment is out-of-service for maintenance and for how long. For many years, plants controlled plant configurations under the Technical Specification requirements. In addition, some plant modes (e.g., shutdown) had few Technical Specification requirements. In the mid 1990s, the industry initiated a number of efforts to assist plant operators and work planners to identify undesirable plant configurations. These efforts led to safety monitoring tools based on PRAs, which allowed work planners to make informed decisions about the scheduling of concurrent activities. These safety-monitoring tools proved invaluable in helping plants to plan shorter and safer refueling outages and to more effectively perform maintenance with the plant at power.

One example of the insights gained from configuration risk management involved a two-unit PWR site, which had back to back refueling outages on twin units. The first unit performed its outage in approximately 35 days. The second unit, performing essentially the same outage plan, managed to complete their outage in only 32 days. However, because of the risk management insights gained in the performance of the first outage, the second unit was able to complete its outage with a total risk that was roughly 22% lower than the first unit, even though the outage was almost 10% shorter.

It is now commonplace for plants to use risk monitoring tools to identify on an on-going basis what the configuration risk levels are and what key activities are being performed. Daily status meetings, plant television monitors and placards at the plant access points are used to alert plant personnel. This communication of risk further ingrains risk management into day-to-day activities at the plant.

5.4 Regulatory Mandated Risk-Informed Applications

The NRC has long considered risk insights in their regulatory processes. A number of regulatory changes have occurred as a result of the insights gained in the performance of PRAs. This section provides a brief overview of some of the more significant risk-informed applications.

Station Blackout Rule

Although the term risk-informed was not coined until the mid-1990s, the Station Blackout Rule (10CFR50.63) was clearly a risk-informed regulatory change in 1988. Station Blackout is a condition in which the plant is without AC power on the buses providing power to safety related equipment. Without AC power, many of those systems are unable to perform their safety function. Plant-specific PRAs performed in the 1980s repeatedly identified station blackout as one of the higher risk contributors using data from actual plant experience with loss of offsite power and emergency diesel generators.

The purpose of the Station Blackout Rule was to assure that plants had an adequate capability to cope with an extended loss of all offsite power. This capability to cope could be provided by assuring high reliability of onsite emergency AC power sources (typically diesel generators), providing additional AC power sources, and/or assuring that plant systems could be assured to operate in a blackout condition for an extended period of time. Each plant was allowed to assess their ability to cope with an extended loss of offsite power based on their own plant unique features. Some plants decided to install additional emergency AC power supplies, others provided assurance of existing plant capabilities. The NRC's assessment of the effectiveness of the Station Blackout Rule estimated that on the average the risk of core damage due to a station blackout was reduced by roughly a factor of 4 across the industry. The impact of changes varied widely from plant to plant. One plant that installed two additional diesel generators found over a factor of four reduction in their total internal events CDF.

Anticipated Transients Without Scram (ATWS) Rule

An ATWS is a plant shutdown event followed by failure of the reactor trip function. This unlikely event would simultaneously cause high reactor system pressure that challenges system integrity, heat removal requirements far in excess of decay heat from a shutdown plant, and a reactor that must be shut down and kept sub-critical. NRC issued its ATWS Rule (10CFR50.62) in 1983 to reduce ATWS risk by 1) reducing anticipated transient frequency, 2) improving the reliability of the reactor trip function, and 3) enhancing plant mitigation if the above preventive measures fail.

We do not have PRA results for ATWS CDF risk before the Rule, but the NRC estimates that it was, on average, more than ten times greater than it is today. Furthermore, most of the benefits are derived from reduction of the anticipated transient frequency; that is, automatic reactor scrams and turbine trips. The next most significant benefit came from improved scram function reliability as a result of better monitoring and maintenance of trip breakers. The least significant contributor was enhanced ATWS mitigation capability associated with new mitigation systems.

The nuclear plant PRAs verify this improvement. The original IPE models reflected some of the changes in-place at the time. At that time, eleven PWR units and eleven BWR units analyzed ATWS to be among the three highest risk initiators. Today, only one PWR and five BWR units list ATWS among the top three risk contributors. Furthermore, the PRA enables owner/operators to monitor the risk level from ATWS as equipment reliability and fuel content (both important to ATWS risk) change over time.

Maintenance Rule

In July 1996, the Maintenance Rule (10CFR50.65) went into effect. The Maintenance Rule was one of the first risk-informed, performance-based regulations promulgated in the U.S. The Maintenance Rule requires licensees to a) identify risk-significant systems, structures and components (SSCs), b) establish performance criteria for selected SSCs (generally based on reliability and/or unavailability), and c) evaluate the safety implications of equipment removed for maintenance.

Since its implementation, the Maintenance Rule has had a significant impact on risk management. The introduction of the concept of "risk-significant SSCs" validated the role that PRA could play in identifying safety significance. In addition, it provided a common language for plant and regulatory personnel to

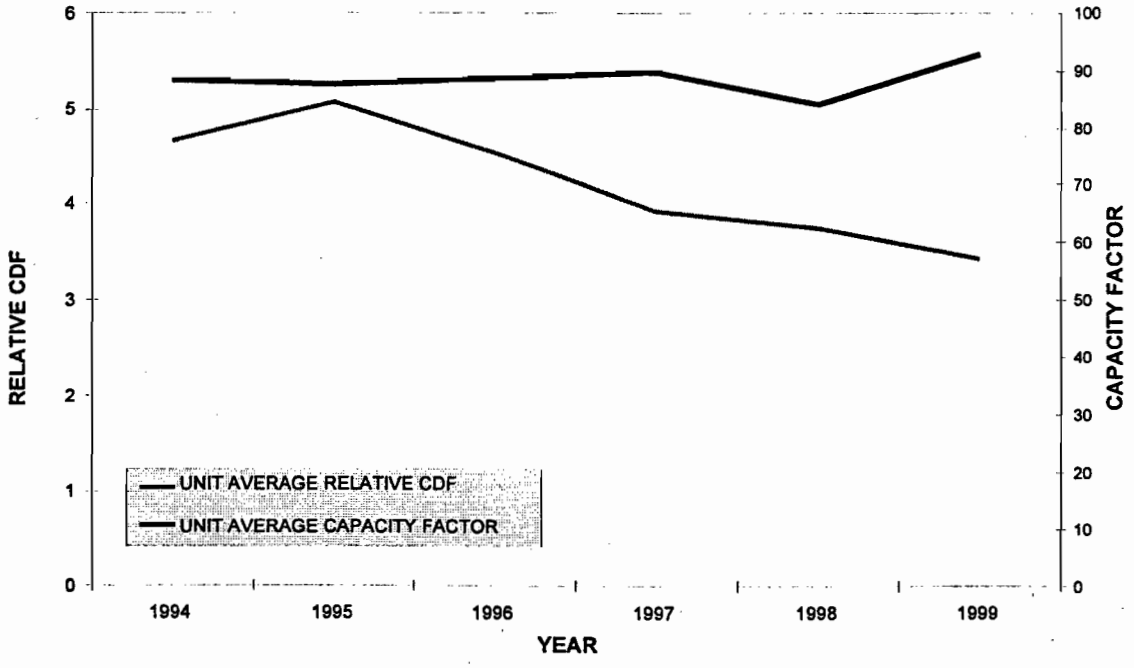
discuss the safety significance of SSCs. That is, SSCs which were considered risk-significant under the Maintenance Rule were considered more important than those which were not.

The establishment of performance criteria for SSCs was tied to reliability and availability data in the PRA. This further tied the PRA to plant operation. If an SSC was going to be removed from service, the implications on the PRA were now necessary to consider.

Finally, the evaluation of safety implications was generally taken to mean the PRA implications. A recent revision to the Maintenance Rule codified this further by requiring licensees to assess and manage any risk increase due to maintenance activities. This requirement has led to the incorporation of risk considerations into the day to day operation of the facility and has led to an improved understanding of risk contributors at all plants by a broad spectrum of plant personnel. It has resulted in risk concepts being used for day-to-day decisions.

In addition, the focus on key risk significant SSCs and the assessment and management of risk implications has, in many cases, led to a reduction in risk at the same time plant performance is improving. Figure 5-1 provides a summary of one utility's four units from just prior to the Maintenance Rule implementation until 1999. This graph shows the relative unit average CDF trend from 1994 to 1999 and the unit average capacity factor for the four units. Over this time frame, the unit average CDF has dropped substantially and the capacity factor has increased.

Figure 5-1
Unit Average CDF and Capacity Factor Post-Maintenance Rule



NRC Oversight Process

In 2000, the NRC initiated a new Reactor Oversight Process which introduces risk-informed performance monitoring and risk-informed inspection findings as part of the oversight process. Previously, licensee performance was evaluated using deterministic indices. This new oversight process allows the NRC and licensees to focus resources on risk-significant issues, rather than expending resources on issues that have limited impact on public health and safety. One key element of the new oversight process is the assessment

of the risk implications of NRC inspection findings. Findings are assigned a color-coded risk-significance (green/white/yellow/red) based on an estimation of the impact on CDF.

Over the first year of the program, many thousands of findings across the industry have been evaluated using this process and only a handful have resulted in a color assignment that was not "green" (non-risk-significant). This new process performs two key functions: 1) it further integrates the concepts of risk into the day-to-day operation of the plant, and 2) it assures that risks will be managed long-term.

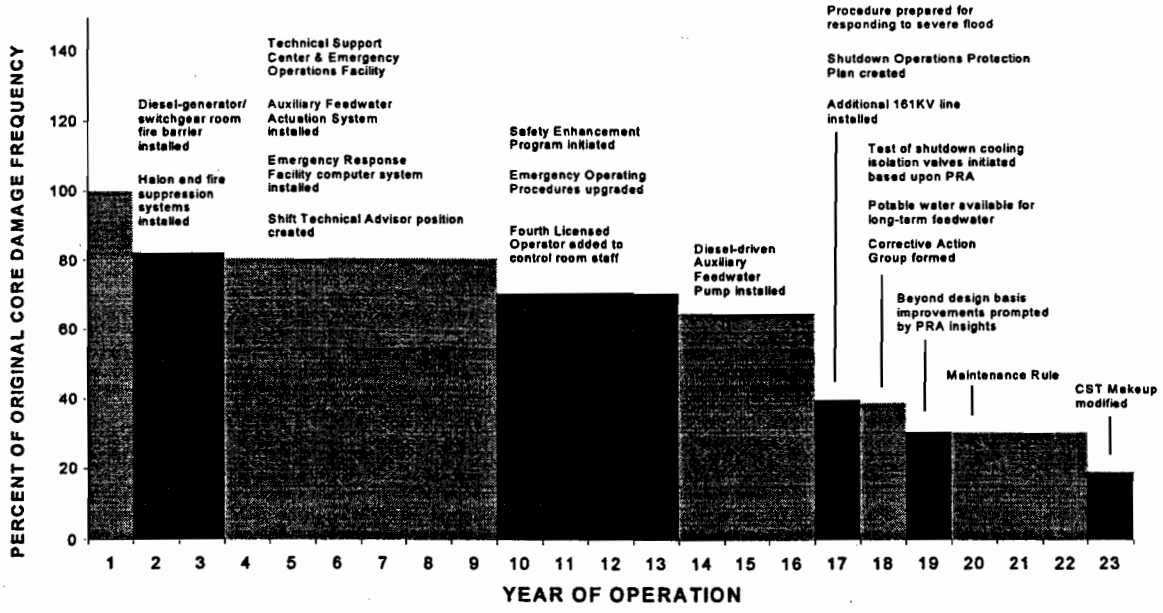
Severe Accident Management

Since the early 1980s plants receiving operating licenses, and now more recently plants requesting license renewals, are required to perform a systematic review of potential severe accident mitigation alternatives. This process involves using a plant-specific PRA for the identification and evaluation of potential plant improvements that could be cost-beneficial. These analyses have consistently identified that expensive plant changes can not be justified, given the level of risk from the current generation of plants. However, on a case by case basis, some plants have identified cost-beneficial improvements, usually in the area of procedure enhancements. One plant performed a systematic evaluation of over 100 different potential plant changes. Two of these changes, both procedures, were found to be cost-beneficial. The net result of these two changes was a reduction in risk of over 30%.

5.4 Cumulative Impact of Risk-informed Changes – A Plant Specific Example

Over the lifetime of the plant, numerous plant improvements, similar to those specific examples described in Sections 5.2, 5.3, and 5.4 above, are made to address regulatory, safety and operational considerations. One plant has compiled a risk history profile which estimates the plant risk profile over the operating lifetime of the facility. The changes in plant CDF are correlated on Figure 5-2 with the plant improvements having the most significant impact.

Figure 5-2
Example Risk Trend Over Plant Lifetime



6. INDUSTRY READINESS FOR SYSTEMATIC RISK-INFORMED, PERFORMANCE-BASED OPERATIONS AND REGULATION

The above sections provide a sampling of data and case studies that illustrate the benefits of systematic risk-informed, performance-based operations and regulations. These examples are representative of significant and widespread safety benefits that have been achieved by the nuclear power industry. The safety levels are remarkable for any complex technical enterprise.

Operating staffs can maintain or improve existing safety levels by risk management. Optimum risk management requires that risk-important equipment and activities receive priority and that risk and performance monitoring be used as indicators of deteriorating conditions and of safety effectiveness. Owner/operators now have the necessary technical capabilities on staff, the calculation tools and models, management awareness and support, and a changed safety culture to capitalize on this technology.

Such a risk management environment will require continuing changes in regulations and attitudes about risk. Regulations for existing plants must be changed to acknowledge and allow residual risk and must allow performance monitoring to verify that the actual risk is acceptable. Regulations for new plants must be risk-informed and performance-based from the start.

With these changes, nuclear power can continue to provide safe, clean, reliable power.