APG REPORT #28

WHERE DO WE GO FROM HERE IN U.S. NUCLEAR SAFETY REGULATION?

A PERSONAL PERSPECTIVE

By

Vojin Joksimovich
Accident Prevention Group

Accident Prevention Group

16980 Via Tazon ■ Suite 110 ■ San Diego, CA 92127 Phone: (619) 592-0189 ■ Fax: (619) 592-0586

REVISION 3
6/7/93

WHERE DO WE GO FROM HERE IN U.S. NUCLEAR SAFETY REGULATION?

A PERSONAL PERSPECTIVE

By

Vojin Joksimovich
Accident Prevention Group

Introduction

This paper was drafted in March with the objectives of: a) sharing the concerns about the state of the nuclear industry, b) searching for a solution, c) incorporating feedback obtained, and d) presenting to key industry players, including the ACRS.

The paper was sent to thirty distinguished individuals in the industry working for the nuclear utilities, NRC, DOE, NUMARC, consulting organizations and academia. The response was overwhelming in terms of encouragement, timeliness, praise for the content, constructiveness and quality of comments received. One reviewer stated: "The subject addressed in your paper has eluded many for decades. It's tough to pin down and tougher still to describe. It is impressive to see an individual tell it from the heart." The paper was revised (Revision 1 dated April 8, 1993) and presented to the NRC's Regulatory Review Group, which amounted to a 3.5 hour mutually beneficial dialogue. Revision 2 (dated May 8) was presented to Consumers Power and valuable feedback was obtained.

In addition to the feedback obtained from the NRC Regulatory Review Group and Consumers Power, additional comments arrived from several nuclear utilities. These, as well as further thoughts have been factored into this Revision 3.

It should be pointed out that the author was an early proponent of risk-based regulation, as exemplified in statements before the Lewis Committee in 1977, Udall Committee in 1978, AIF Safety and Licensing Forum in 1979, and ACRS in 1981. Co-authorship of NUREG-1050 should also be mentioned.

A Historical Perspective

Throughout my 30-odd year career in the world nuclear industry, the industry has been preoccupied with the hardware, QA/QC and engineering aspects, almost to the point of obsession. As a good illustration, in the aftermath of the TMI accident, which was not so much with the hardware as with how the hardware was employed or not employed, thousands of hardware changes were proposed and many, of peripheral public risk reduction impact, were implemented, costing the rate payers billions of dollars. One of the conclusions of the Kemeny report (Kemeny, 1979) was that the

fundamental problems were people-related problems and not equipment problems. The TMI action plan even applied to HTGRs. Nuclear safety expertise was pretty much equated with knowledge of structures, systems and components.

Human factors, or ergonomics, as a discipline was born in other industries, such as aircraft and aerospace. A technology transfer workshop originated by the White House in the aftermath of TMI and sponsored by ANS/IEEE provided most of the new considerations, such as the control room design review and control room staffing.

Although the landmark Reactor Safety Study (RSS) or WASH 1400 was completed in 1975 and unambiguously demonstrated that the bulk of risks associated with operation of nuclear power plants (NPPs) were associated with severe accidents, *i.e.*, beyond design basis, a regulatory emphasis on severe accidents was painfully slow to phase in. Until TMI, the findings of the study were practically dismissed by the NRC. Even in the aftermath of TMI, plant-specific PRA studies were only requested for high population sites in order to establish risk significance of some exotic hardware solutions such as core ladles. The utility industry embraced PRAs primarily in order to contest such non-meritorious, expensive backfits, which would have shut down many plants, and certainly Big Rock Point (BRP). Appendix A, (reproduced from Blanchard, 1985) presents a remarkable display of rationality and transparency, for uses of PRA in the regulatory process. Another BRP paper (Donnelly, 1991) successfully addressed two human dominated regulatory issues: shift staffing and control room design review. The plant continues to run, and it is planned to run through the year 2000. The NRC's severe accident policy was not promulgated until 1985 and the generic letter for plant-specific PRAs (GL 88-20) was not issued until 1988.

Well before TMI, the NRC instituted a requirement for licensing reactors operators, *e.g.*, part 55. Licensing operators only was not sufficient for exercising regulatory control over a complex NPP organizational structure. The inspection program was established first and then a regulatory activity called SALP (Systematic Assessment of Licensee Performance) was born in order to gauge how well a utility was doing in operating a plant by virtue of auditing seven functional areas. SALP is a costly, extremely subjective and judgmental process with no apparent scientific basis. It appears not to be risk-based, and apparently was not a product of profound research. NUMARC (Colvin, 1992) states: "The SALP process is subjective, establishing grades upon opinion rather than on established and consistent criteria. It allows five separate NRC regions and individuals within each region to, in effect, impose their individual views on licensees." The NRC is currently in the process of revising SALP, with final proposed changes forwarded to the Commission (Russell, 1993).

TMI also gave birth to INPO, which in turn gave dignity to plant operations as a discipline. INPO developed training programs not only for the licensed operators, but also established a system of peer reviews and inspection of operations, and in general did a lot of exhorting to excellence. INPO and SALP approaches observe outcomes and conclude that some of them need improvement and some are good. In my opinion, they do not address a central issue of how NPPs should organize and manage their resources to accomplish an efficient, safe and optimal-cost plant. There is no scrutable

basis for design of a NPP organization and again, there is no visible risk-based focus of nuclear safety operational considerations, such as prevention of severe accidents. Admittedly, in view of confidentiality, I have had no access to INPO documents.

Despite the fact that NPPs now generate in excess of 20% of the nation's electricity, and despite the fact that PRA is now a mature discipline (with accompanying abuses, of course), we have not been able to sufficiently factor risk perspectives either into nuclear regulation or NPP operations. The industry has not coordinated a concerted effort. Fire drills and immediate "provide what I want to prove" approaches result in replication rather than collaboration. The "compliance mindset" coupled with PRA experts oversell of PRA capabilities, in particular when it comes to validity of bottom line values, resulted in a stalemate.

A smooth transition from traditional design and construction activities to operations has not been made yet. As David Ward has eloquently stated, "When there is a disconnect between what is needed and what we know how to do, the latter wins. A man with a hammer sees everything as a nail." (Ward, 1992).

Plant operations have to be seen as a collection of systems, human actions and process requirements in a highly interactive mode, as opposed to individual rule compliances or non compliances. Making this, what appears to be a revolutionary change from binary (OK-Not OK) compliance thinking to a highly interactive systems performance perspective, and its associated reduction in variabilities seems to be the underlying cultural hurdle the nuclear industry must overcome.

A Perspective on Status of Nuclear Safety

One can safely state that there is a general consensus amongst nuclear safety experts that there is more than sufficient hardware in existing NPPs. The plants are well designed to withstand natural phenomena such as earthquakes. In fact, they are over-designed. The Shoreham study (Shoreham, 1985) discovered that, with the exception of ceramic insulators, beyond the control of a NPP, the first component to fail required an earthquake four times safe shutdown earthquake (SSE). Fire protection despite recent thermal lag issue, but in view of Appendix R attention, is more than adequate. All in all, the existing hardware is good enough. Only marginal further gains could be made in this area, despite apparent imbalances in the design. Any appreciable gains can only be achieved with advanced designs like ALWRs and HTGRs. Many PRAs/IPEs corroborate this conclusion. Of course, this may not be necessarily true for every single plant in the country, but the existing IPE process should reveal major outstanding design inadequacies.

Since TMI, readiness of operating crews to respond to complex accident scenarios has been greatly enhanced. Simulator training and emergency operating procedures are probably the most instrumental in this success story. However, there is no room for complacency and more needs to be done, not in terms of quantity, but quality of training. Current training demands are excessive. The simulator offers much more before it reaches its full potential.

The ORE (Operator Reliability Experiments) project (EPRI NP-6937, 1990/91) jointly sponsored by EPRI and six U.S. nuclear utilities, collected data at six full-scope control room simulators. The project encompassed simulation of 43 plant-specific accident scenarios, involved 93 operating crews, focused on 117 human interactions, and resulted in more than 1,000 data points. This constitutes the largest operator action simulator data in the world. Subsequently, EPRI sponsored development of an application of ORE methodology for plant-specific PSAs or IPEs (EPRI NP-6560L, 1989). In order to facilitate automatic simulator data collection, a tool named OPERAS (Operator Reliability Assessment System) (Spurgin, *et al.*, 1992) was developed.

The measurement techniques developed and applied in these and other projects contain a potential for answering conclusively fundamental safety questions regarding operator readiness, training effectiveness; optimal crew composition on case-by-case basis to safely manage the plant, etc. Two examples provide a minor illustration of the potential of this methodology (Figures 1 and 2). Figure 1 illustrates an example of an anomalous crew detection (Molden, 1989) through measurements, which was elusive to human observers and was explained upon examination of video tapes; while Figure 2 illustrates a simulator data based PRA application for three types of BWR and PWR human interactions. Regretfully, institutional obstacles and inertia associated with reluctance to accept measurements rather than educated guesses, have thus far prevented wider use of these techniques for both training and PRA/IPE applications. As a result, PRAs/IPEs typically employ generic operator action guesses rather than the simulator data. Paradoxically, ORE style data collection has been completed at the PAKS VVER simulator in Hungary, and is being interpreted for use in the PAKS PRA.

What is not good enough is our understanding of plant operations and operational risks. We are reluctant to apply plant operational risk models capable of simulating NPP risks vs. time, despite existence of the basic technology (Vesely, 1993). The models that we do have show that core damage frequencies (CDF) can undergo large changes over time due to changing plant hardware configurations. Figures 3 and 4 (reproduced from Specter, 1993) show quarterly analysis reflecting actual operating plant configurations as well as plant configurations yielding very high CDF spikes. Most dramatically, there appears to be a strong correlation between many high risk configurations and precursor events (Vesely, 1992). The drifts in CDF attributable to human reliability and organizational factors considerations are not even modelled yet. On the other hand, we are aware that essentially a single competent and committed individual in an executive position can make a vast difference in fostering a safety culture, as exemplified at Turkey Point (O'Neill, 1992).

In the aftermath of Chernobyl, the International Atomic Energy Agency's International Safety Advisory Group (INSAG, 1991) has issued a series of reports dealing with the safety culture, intended for use by government authorities and by the nuclear industry and its supporting organizations. While copies of the booklet were distributed to all utility CEOs, this noteworthy literature package made very little observable impact in the U.S. that I am aware of. Relatively recently, the Agency issued ASCOT Guidelines -- "Guidelines for Self Assessment of Safety Culture and for Conducting a Review, by the Assessment of Safety Culture in Organizations Team".

The USNRC has an ongoing comprehensive program in human factors. One area of research is directed towards assessing the influence of organizational factors and management on NPP performance. APG, as a participant in the program, is disappointed with the slow progress made. Institutional factors (*e.g.*, NRC vs. NUMARC dispute, NRC's own prejudices) are a significant element in this disappointment.

The bottom line is that our understanding of the safety culture, not to mention the nuclear risk culture, is at a rudimentary level, which I would characterize as a great concern. This should be examined using perspectives derived from analyses of catastrophic accidents (such as Chernobyl, Bhopal, Challenger, Amoco Cadiz, Piper Alpha, Exxon Valdez), which show that these accidents may be characterized by four broad categories of root causes (abbreviated as "4M"):

- **Machine** (design with its basic flaws)
- **Milieux** (natural phenomena, operational conditions, political environment, commercial pressures, etc) providing triggering events, and
- **Man** (operating crew response)
- **Management** (basic organizational safety culture flaws)

Strong management can minimize the contribution of machine, milieux and man to nuclear operational risks. One way management can have this powerful positive influence is through establishment of a proper safety and risk culture (Joksimovich, 1992).

Repercussions

No other industry has invested more resources to safety than the nuclear industry. For this large investment, the industry has achieved a remarkable safety record. Nevertheless, there is no room for complacency. Despite the fourteen years of major accident free record, our understanding of operational risks to reflect various plant hardware configurations, human reliability and organizational factors needs to be enhanced. A recent Stinson paper (Stinson, 1993) states: "Many plants evolved from construction to operations with little consideration given to development needs of key personnel in their new roles. Given focus on technocracy, there was no resultant cultural environment that emphasized the value of interpersonal skills development nor were there rewards for leadership or management expertise." Therefore, the emphasis has to shift from traditional engineering considerations, and the industry has to do what needs to be done, as opposed to what the industry traditionalists know how to do today.

Rising O&M costs, largely attributable to regulatory requirements and how the utilities have responded to them, are driving the industry right into the ground. To quote from the 1989 Regulatory Impact Survey: "NRC so dominates licensee resources through its existing and changing formal and informal requirements that licensees believe that their plants, though not unsafe, would be easier to operate, have better reliability, and

may even achieve a higher degree of safety, if licensees were freer to manage their own resources." The nuclear utilities cannot economically compete with fossil fuel plants and other sources of electricity. Permanent shutdowns of Yankee Rowe, San Onofre Unit 1 and Trojan clearly signal the magnitude of the problem. The crisis boils down to an issue of how to maintain or enhance (where it might be appropriate) nuclear safety at sustainable reduced costs in an acceptable regulatory framework. Hence we have to learn how to maintain nuclear safety at reduced cost. This leads to Risk Based Regulation (RBR).

Risk-Based Regulation and Management

The only way to succeed is to free up NPPs from incurring costs from regulatory and INPO driven activities which do not contribute in any sizable manner to maintenance or enhancement of acceptable plant risk levels. A good example would be a requirement for the integrated containment leak tightness testing. Reducing frequency of this test from three to, say, ten years, would most likely result in risk differential of zero. The NRC's Regulatory Review Group (Gillespie, 1993) is currently reviewing the regulations, *i.e.*, parts 21, 26, 50 and 73, from the standpoint of streamlining, eliminating inconsistencies, questioning effectiveness of plans such as fire protection, reporting requirements, etc., as well as introducing risk based regulation, *i.e.*, 50.66 (maintenance), Appendix B (quality assurance), 50.55a (IST/ISI), 50.36 (Tech Specs), 50.59 (Design/FSAR). The NRC's research showed the U.S. is behind the U.K. and Scandinavian countries when it comes to risk based usage in regulation (Figure 5).

Risk-based regulation, *i.e.*, a compendium of regulatory implementation guides should be explicitly based on risk analyses which are traceable and scrutable. It needs to be, however, pointed out that even if the regulators and licensees were completely competent in the practice, risk quantification is still an art as well as a science, and the general public's lack of appreciation of relative risk concepts is an unfortunate impediment to the pace with which progress can be expected in public understanding. Nonetheless, we can achieve a goal of rational and transparent regulation if we devote appropriate resources to exploiting the full potential of PRA techniques which are by and large currently available, but are only in limited use both by the regulator and the nuclear utilities. Vesely has convincingly illustrated existence of a technology consisting of ten NUREGs (Vesely, 1993) summarizing the work performed over eight years and focusing on:

a) Risk-based surveillance test intervals,
b) Risk-based allowed outage times,
c) Risk-based management of components being down a given time,
d) Reliability and risk-based maintenance prioritization and optimization,
e) Risk-based management of aging effects.

Like EPRI-sponsored human reliability technology and IAEA sponsored safety culture literature referred to earlier, this NRC-sponsored technology is virtually untapped. Why is that? This paper raises the issue, but does not attempt to provide a full answer.

Regulatory requirements should be distributed according to risk significance. Herschel Specter has illustrated beautifully how it could be applied in the maintenance rule case (Specter, 1993). In another paper (Specter, 1992) he illustrated the example of costs associated with various non-safety vs safety related components such as with high ratios such as: $242.44 vs $4,447.00; $29,000 vs $66,800; $207.00 vs. $7,548, $1.35 vs $21.12, etc. New York Power Authority paid $313.00 for a single hex socket set screw which can be bought in a local hardware store.

In addition, I advocate that greater self-reliance and more self-regulation through instillation of enhanced safety and risk culture via advanced self-assessment programs should also be a key ingredient of RBR, which may or may not be a part of the license similar to integrated living schedule, which is a part of BRP's license.

A good example for an advanced self-assessment is an integrated risk management program (IRMP). IRMP is a concept similar to total quality management (TQM) which assures that goods and services delivered to clients meet the established quality standards. Many U.S. companies are embracing the TQM concepts as one means of competing in global markets. It is my creed that operation of a NPP with an appropriate safety and risk culture assured via an IRMP will be an efficient, reliable and optimal-cost plant.

IRMP

Risk management is defined as the decision making process to minimize potential losses. Typically, risk management is accomplished by virtue of exercising a risk model of a specific plant and weighing the costs, benefits and risks of available options for achieving risk control. ***Degree of success is dependent on the quality of the risk model. If the risk model is geared towards the plant hardware aspects only, then its usefulness is confined to identifying plant configuration vulnerabilities, but is not necessarily successful for all plant operational considerations.*** For the latter, the risk model has to be capable of simulating NPP risks vs. time and be capable of accommodating human reliability and organizational factors, *e.g.*, safety and risk culture.

A number of utilities have developed risk management programs primarily geared to hardware considerations. Hence, I would not call them integrated since they represent a suboptimal case. To my knowledge, Yankee Atomic has probably the most advanced program in the industry (Yankee, 1991). A striking example was the use in closure of NRC's severe accident policy issues, *i.e.*, IPE, IPEEE, Containment Performance Improvement (CPI) and Accident Management (AM). NorthEast Utilities is another industry leader and a staunch advocate of using living PRA in decision making (Bonaca, 1991).

Figure 6 depicts an IRMP framework. The left-hand portion of the chart represents the areas where organizational factors, (behavioral science) come into play in the complex interactions of organizational units and people (organizational variables and individual variables). External influences of regulatory pressures and business on a

nuclear utility, as well as internal corporate culture affect the policies and practices of the organizations, including its ability to foster an effective safety culture. ***These external influences and how the utilities responded to them have driven O&M costs beyond what the market is willing to bear***. The right-hand side of the chart illustrates that the organizational factors influence the reliability of plant personnel (HRA), with respect to safe operations and maintenance, which in turn factors into components of plant safety and reliability (PRA). Behavioral science PC-based instruments listed on the chart, like ACUMEN, represent a selection of tools routinely employed by Management Analysis Company in San Diego.

Figure 6 also demonstrates that utilities cannot successfully manage nuclear risks independent of common business issues. It is imperative that a more holistic view of plant management responsibility be seen. Land and Sancic's paper (Land, 1990) reflects realities of plant decision making. Plant managers must successfully balance public safety, personnel safety, economic performance, personnel productivity and regulatory impact. The scope of this paper is, however, confined to nuclear risk management.

IRMP Principal Elements

IRMP's principal elements should be entirely plant specific. On a generic basis, and as I currently envisage, IRMP could consist of the following principal elements (Figure 7):

- Organizational nuclear safety/risk culture initiatives
- Integral plant-specific risk assessment
- Operational plant-specific risk model
- Establishment of operational plant risk limits
- Use of operational plant risk model for trending purposes
- Plant operational event analyses (feedback)
- Emergency planning
- Internal or external risk based audits

Organizational Nuclear Safety/Risk Culture Initiatives

In my Monterey paper (Joksimovich, 1992) I have dealt with the subject of nuclear safety culture in nuclear utility operations. The utility CEO needs to explicitly endorse and be active in various safety culture initiatives. An example of one utility's safety culture initiatives is reproduced here as Appendix B. Powerful examples of a commitment to nuclear safety are the existence of independent safety oversight or risk group reporting directly to the CEO, and a requirement for submittal of annual nuclear safety assurance reports.

However, in dealing with the subject of safety culture, it became apparent that a risk culture as a subset of the safety culture has received little to no attention thus far. In a PSA '93 paper (D. Okrent, *et al.*, 1993) the authors have included, appropriately, risk assessment in their deep technical knowledge distribution matrix (Figure 8). For each position the level of knowledge was determined based on a three point scale:

1-passive knowledge, 2-working knowledge, and 3-detailed knowledge. Currently, knowledge of risk assessment is confined to a small specialized group within a utility. A few managers might be able to respond to a fundamental risk question such as, say, what are dominant contributors to risk for their plant. Instilling risk culture amongst the utility management personnel should become a part of the management training. Furthermore, every employee of a NPP should receive a proper dose of risk training. Ideally, each one should understand how his/her job affects NPP safety and what events might transpire if they err.

Integral Risk Assessment

Here we are dealing with the plant-specific PRAs/IPEs as we know them, consisting of identified and quantified thousands of accident scenarios or sequences. A bottom-line estimate such as CDF is the sum of all sequences analyzed, each one providing an increment in frequency, consequences, and therefore, risk. Such a process is invaluable in evaluating the NPP design and identifying the plant vulnerabilities. In the integration process, parameters such as component failure rates or unavailabilities are treated as time averaged values. This approach doesn't evaluate importance of several components unavailable at the same time.

Integral PRA/IPE models generate lists of risk significant systems, components and operator actions. These lists can be successfully employed to generate grading scales for several NPP activities subjected to regulations such as quality assurance, maintenance and in-service inspection. Figure 9 displays a risk-based maintenance process flowchart. However, integral PRAs/IPEs do not account for the actual measured readiness of plant-specific operating crews to respond to an accident scenario. The treatment of nuclear reliability by "handbook" methodology fails to capture possible operating crew performance given an accident scenario. In addition, organizational factors are typically not modeled. All in all, integral PRAs are invaluable for assessing the plant design aspects but not necessarily operational ones.

Operational Risk Model

For plant operational considerations, the above listed shortcomings need to be overcome. In the last several years, a number of NRC sponsored studies focused on operational aspects and technical specifications in particular, *e.g.*, NUREG/CR-5925 (1992), NUREG/CR-5641 (1991). The operational risk model is based on an integral plant-specific PRA/IPE, but modified to satisfy needs of the technical specification applications. The model needs to be more detailed than in a typical PRA/IPE to accommodate potentially significant component outage combinations which may not be important for the purpose of an integral PRA. Conversion of an existing PRA/IPE into a model allowable for real time technical specification calculations addresses the following issues: a) methods for reconfiguration of the plant model for optimum calculation times, b) an approach for explicit treatment of operator recovery actions, and c) recommendation on detailed modeling of systems normally not included in a PRA/IPE.

In addition, the operational risk model needs to address adequately operator reliability and organizational factors influences. No such explicit model has yet been developed to our knowledge. Figure 10 displays an operational risk management flowchart.

Operational Risk Limits

For an effective management of plant risks, a set of operational risk limits needs to be established. Appendix C provides an excellent self-explanatory example developed and in use by NorthEast Utilities.

Another risk control mechanism is to focus on ΔR, t and $\Delta R\,t$. ΔR is the risk increment over some acceptable base line value, say CDF - 10^{-4}/year, which could be associated with a change in monitored plant performance, while t is the time during which ΔR drift exists.

Risk Trending

This is a crucial part of any risk management program with both safety and availability implications. In the past, this was primarily done intuitively and judgementally.

Virginia Power Company (Cross, 1991) has developed and implemented a system/component trending approach based on technical specification-limiting condition of operation (LCO) and action statements (AS) total hours and a breakdown by system and component. The premise is that limiting amount of time key safety systems are out of service will: a) reduce overall plant risk level and b) improve plant availability. One year total for AS hours for both Surry units was 8869 hours. The dominant contributors (32%) were: service water system (1430 hours) and ventilation system (1403 hours) which are interrelated, *i.e.*, service water (SW) supplies cooling to the ventilation system (V). SW breaks down into dominant components; emergency pumps (38% or 545 hours) and discharge tunnel radiation monitor (52% or 747 hours). This is a commendable approach. Virginia Power is aware that using PRA is a better approach and has expressed plans to switch downstream.

In our view, operational risk model is a tool for assessing CDF vs. time as illustrated in notional Figure 11. The upper part of the figure shows how the number of recorded failures per year of some components, say service water pumps, may vary around the historical average used in integral PRA/IPE. If the failures were being trended out, they might reveal an increase in failure frequency as a result of some organizational factor in the maintenance department.

Similarly, the upper right of Figure 11 depicts the decrease in measured unreliability of control room crews due successively to positive OFs, *e.g.*, steps taken to improve EOPs and/or training until the time, say, of training budget reduction, after which the crew unreliability begins to increase. The lower portion of Figure 11 depicts how recognition of the time dependency in databases should be reflected in estimated CDF for the plant.

In order for risk trending activities to be based on high quality data, computerized data collection systems have to be installed, not only for monitoring hardware performance, but also for monitoring operating crew performances, as well as measuring organizational safety culture trends. Such systems employing PC technology are commercially available.

Operational Feedback

The industry has performed remarkably well in this area in the aftermath of TMI, *e.g.*, LERs, plant specific event reports, deviation reports, root cause analyses, etc. There is clear evidence that utilities are reviewing events of others and disseminating to staff, but probably more needs to be done. I have personally studied how one utility performs these types of analyses and was very satisfied. Our experiences in the ORE project reconfirm the importance of feedback from operations and training to continually improve emergency operating procedures (EOPs). The existing processes for all forms of operational feedback simply need to be perfected from the standpoint of focusing on risk perspectives.

Emergency Planning

This is another success area in the aftermath of TMI. In my judgement, we are not at the point when we can claim that the risks from NPP operations are so low that emergency planning is unnecessary. However, there is room for improvement (*e.g.*, more of realistic scenarios) and a relaxation by virtue of reducing frequency of the drills. For example, cost savings by bi-annual drills, as opposed to quarterly drills at San Onofre could be reallocated to programs having higher risk reduction potential. Quarterly drills could be compared with too frequent testing of diesel generators, resulting in wearouts.

Risk-Based Audits

Audit provides eyes and ears to nuclear utility management in order to assure a successful IRM. It could be internally or externally conducted. Existing SALPs and INPO evaluations contain only remote and conjectural relationship to plant risk control. When I had an opportunity to ask an NRC Regional Director, thoroughly experienced in SALPs, "What is the relationship between SALPs and risk control?", the response was "There is none, but there should be". Of course there should be, and we should get busy initiating research and a reform in this area. It is grossly overdue.

As a starter, organizational units and programs important in an IRMP, either resulting from regulatory imperatives of good practices should be identified. A rough illustration is provided in Figure 12.

Our experience in working with a number of utilities is that there is a tremendous fragmentation among such programs with a lack of appreciation of the interrelation of one program to the other; in particular, with regard to nuclear safety and risk. A good example being a lack of integration between PRA/IPE human factors/reliability

and training activities. Figure 13 illustrates an integrated approach. Close integration of these activities will not only enhance safety, but also substantially reduce costs, and it is up to an audit to identify weaknesses and propose corrective actions on the utility management, both from the standpoint of risk control and cost reduction.

Proper Regulator Role

The forgoing places greater emphasis on self-awareness and self regulation. What then should be the proper role of the regulator? The regulator should have no other goals than focused attention to nuclear safety. However, the nuclear utility has ultimate and undivided responsibility for nuclear safety. I believe that the USNRC should assume more of the stance taken by regulators in the U.K. and in Sweden rather than the generally confrontational and mutually suspicious relationship that currently exists. The operating utility and regulator assume joint responsibility for the health and safety of the public in a system of "checks and balances"; when difficult problems arise, they are solved together for mutual and public good.

In transition to risk based regulation, the existing regulatory fabric should be streamlined to focus on substantive nuclear safety rather than numerous marginal and peripheral issues. It is expected that the report to be submitted to the Commission on July 30th by the NRC's Regulatory Review Group will contain a large number of recommendations aimed at achieving these objectives. It will be up to the utilities to take the advantage of the favorable climate to be created and come forward with a number of RBR initiatives. My concern is that the NRC may not be prepared to respond similar to the situation regarding use of completed IPEs.

For success of the IRMP approach outlined above, the utility must be assured that it will get proper credit for being innovative and be allowed the responsibility of virtual self-regulation. The regulator and utility would establish the framework and guidelines for self regulation using the IRMP. The NRC would perform initial review and periodic audits of the self-regulation process, in an advisory role, taking more intrusive actions only when audits or agreed-upon performance indicators warrant such actions.

The initial review of the utility's IRMP would provide reasonable assurance that the programs and organization at the NPP would achieve the objectives as outlined above. This could involve a review of the role and authority of the "risk manager" function, the technical knowledge and risk-culture credentials of the key plant personnel.

Another function of the NRC could be to review and approve the baseline and updates to the "living PRA". The review should not be as exhaustive as for a traditional SAR but only to judge reasonableness of results, data, methods and assumptions. As the backbone of its own risk-based decision making, the utility has a vested interest in producing a realistic appraisal of their NPP's risk. It is not, in our opinion, necessary for the NRC to have to recalculate every number nor perform quality checks for every computer program used to produce the PRA/IPE.

A role for the NRC research should be to support the "checks and balances". Regulatory paradigm might be to:

1. Develop generic guidelines for an acceptable IRMP program including programs and organizational elements, perhaps including recommendations for levels of nuclear safety knowledge for all persons having influence on plant O&M, from corporate decision-makers to plant personnel.

2. Develop or list PRA elements deemed acceptable for supporting an IRMP in self-regulation (*e.g.*, which PRA modeling techniques or human reliability analysis techniques are acceptable; how plant-specific equipment and human reliability databases should be accumulated and documented and acceptable methods for utility's benchmarking of PRA software).

Without stultifying innovation by the utilities, NRC research could provide scientific basis for the key elements and sub-elements of IRMPs.

Corollary - Ten Assertions

1. No other industry has invested more resources in public safety than the nuclear industry. O&M costs largely attributable to regulatory requirements and how the utilities have responded to them, have escalated to unacceptable levels and are driving competitiveness of nuclear utilities right into the ground. Long-term sustainable and manageable cost reductions are imperative for saving the nuclear option.

2. For this large investment, the industry has achieved a remarkable safety record. Nevertheless, there is no room for complacency; the level of safety achieved has to be maintained and continuously looked to be enhanced.

3. The nuclear industry worldwide has been preoccupied with the hardware to the point of obsession. TMI action plan alone resulted in thousands of hardware changes costing the rate payers billions of dollars. As a result, existing hardware is good enough. There is now clear recognition that many hardware considerations, initially incorporated into the design or later backfitted, as well as elaborate plant security arrangements, are of peripheral impact to public risks associated with NPP operations.

4. Since TMI, readiness of operating crews to respond to complex accident scenarios has been greatly enhanced. Simulator training and emergency operating procedures are probably the most instrumental. However, more needs to be done, not in terms of quantity, but quality of training. The simulator offers much more before it reaches its full potential.

5. With almost all NPPs operational, the emphasis has to shift from traditional engineering considerations into entirely operational ones. In order to maintain and enhance the existing level of safety, our understanding of operational risks

has to be vastly expanded. Plant operations have to be seen as a collection of systems, human actions and process requirements in a highly interactive mode which requires a cultural change in the industry. The "4M" aspects, discussed briefly in this paper, should receive due attention. Core damage frequencies can undergo large changes over time due to changing plant hardware configurations, human reliability and organizational factors.

6. Full benefits should be derived from currently under-utilized and sufficiently in-depth researched disciplines such as PRA in both integral and time-dependent mode, human reliability and safety culture.

7. Risk-based regulation and plant management, as advocated in this paper, is an answer. Greater self reliance and more self regulation through instillation of enhanced safety and risk culture via advanced self assessment programs should be key ingredients. A good example for an advanced self assessment program is the Integrated Risk Management (IRMP) proposed in this paper.

8. Risk technology applications as proposed by the NRC's Regulatory Review Group represent a step in the right direction. Subsequently, the NRC should gear up its resources to respond expeditiously to nuclear utility initiatives. Furthermore, a regulatory culture reform will be needed to reflect some points made above.

9. Regulatory culture reform should address two fundamental issues: the proper role of the regulator, *i.e.*, cooperative, like in many European countries vs. competitive, and change of binary (OK/Not OK) compliance thinking to a highly interactive systems performance perspective and its associated reduction in variabilities.

10. A massive instillation of risk education in the whole industry via management and personnel training has to be initiated, and the sooner the better. In addition, rule-based culture has to be substituted with knowledge-based culture. Regulatory and utility-sponsored research must continue with emphasis on the human and organizational factors in particular.

REFERENCES

[Blanchard, 1985] Blanchard, D., "PRA and Regulation", USIR/NRR Seminar, September, 1985.

[Bonaca, 1991] Bonaca, M.V., Editor, Living Probabilistic Safety Assessment for Nuclear Power Plant Safety Management, NEA, 1991.

[Colvin, 1992] Colvin, J.F, to I. Selin, NUMARC letter dated October 20, 1992.

[Cross, 1991] Cross, R.W., "System/Components Trending for Management of Overall Plant Risk", ANS 15th Biennial Reactor Operations Division Topical Meeting on Reactor Operating Experience, Seattle, WA, August, 1991.

[Donnelly, 1991] Donnelly, P.M. "Two Successful Applications of Probabilistic Risk Analysis to Address Regulatory Issues", Risk Management - Expanding Horizons, 1991.

[EPRI NP-6937 1990/1991] Spurgin, A.J., *et al.*, "Operator Reliability Approach Using Power plant Simulators, Volumes 1, 2 and 3, EPRI NP-6937 and EPRI NP-6937L, Electric Power Research Institute, Palo Alto, CA, 1990 and 1991.

[EPRI NP-6560L, 1989] Spurgin, A.J., P. Moieni, and G.W. Parry, "A Human Reliability Approach Using Measurements for Individual Plant Examinations, EPRI NP-6560L, Electric Power Research Institute, Palo Alto, CA, 1991.

[Gillespie, 1993] Gillespie, F.P., "Briefing on Progress of NRC Regulatory Review", March 1993.

[INSAG, 1991] International Nuclear Safety Advisory Group, Safety Culture, Safety Series No. 75-INSAG-4, IAEA, Vienna, 1991.

[Joksimovich, 1992] Joksimovich, V., "Safety Culture in Nuclear Utility Operations", 1992 IEEE Fifth Conference on Human Factors and Power Plants, Monterey, CA, June 1992.

[Kemeny, 1979] Kemeny, "The Need for Change: The Legacy of TMI", October 1979.

[Land, 1990] Land, R.E., and Sancic, D., "Value Ranking System for Nuclear Plant Modifications", Nuclear Plant Journal, Sep-Oct 1990.

[Molden, 1989] Molden, J.E., "Research in Operations: Lessons Learned", Proceedings of the Eighth Symposium on Training of Nuclear Facility Personnel, Gatlinburg, TN, 1989.

[NUREG/CR-5641, 1991] Samanta, P.K., *et al.*, "Study of Operational Risk-Based Configuration Control", NUREG/CR-5641, Brookhaven National Laboratories for United States Nuclear Regulatory Commission, Washington, DC, 1991.

[NUREG/CR-5925, 1992] Puglia, B., *et al.*, "Risk-Based Technical Specifications: Development and Application of an Approach to the Generation of a Plant-Specific Real-Time Risk Model", NUREG/ CR-5925, United States Nuclear Regulatory Commission, Washington, DC, October, 1992.

[Okrent, *et al.*, 1993] Okrent, D., *et al.*, "Use of Behaviorally Anchored Rating Scales (BARS) for Deep Technical Knowledge", PSA '93, Clearwater, FL, January 1993.

[O'Neill, 1992] O'Neill, "Thanksgiving at Turkey Point, Nuclear Industry, Third Quarter 1992.

[Russell, 1993] Russell, T.W., "Systematic Assessment of Licensee Performance (SALP)", NRC Staff Presentation to ACRS, April 1993.

[Specter, 1993] Specter, H., "PSA, Calculus and Nuclear Regulation", PSA '93, Clearwater, FL, January 1993.

[Specter, 1992] Specter, H, "Shifting the Regulatory Paradigm", NYPA, 1992.

[Spurgin, *et al.*, 1992] Spurgin, A.J., J. Hallum and J.P. Spurgin, "Operator Reliability Assessment System (OPERAS)", Volumes 1, 2, and 3 EPRI RP-3082-01, Electric Power Research Institute, Palo Alto, CA, 1992.

[Stinson, 1993] Stinson, R.C. and Desmerais, R.A., "ANS Executive Conference, The Management Challenge: Better, Safer, Cheaper Nuclear Power -- Lessons Learned", May, 1993.

[Shoreham, 1985] Joksimovich, V. and Orvis, D.D., "Major Common-Cause Initiating Events Study -- Shoreham Nuclear Power Station", February, 1985.

[Vesely, 1992] Vesely, W., Private Communication

[Vesely, 1993] Vesely, W. "Risk-Based Regulation and Risk-Based Aging Management", The Second International Conference on Nuclear Engineering, San Francisco, CA, March, 1993.

[Ward, 1992] Ward, D., "Do We Need Advanced Humans?", Remarks at conference luncheon, 1992 IEEE Fifth Conference on Human Factors and Power Plants, Monterey, CA, June 1992.

[Yankee, 1991] Yankee Atomic Electric Company, "Applications of Probabilistic Risk Assessment" EPRI NP-7315, Electric Power Research Institute, Palo Alto, CA, 1991.

	CREW #	1	2	3	4	5	6
HI #							
1		1.06	1.11	3.44	0.61	0.81	0.89
2		2.62	1.15	2.48	0.34	0.04	0.56
3		0.40	0.20	2.28	2.97	0.90	0.73
4		1.10	0.83	1.58	0.71	0.92	1.21
5		0.90	2.02	0.09	1.44	1.54	2.17
Average		1.09	1.24	1.84	1.02	0.94	1.08
Standard Deviation		0.53	0.55	0.8	0.57	0.31	0.32

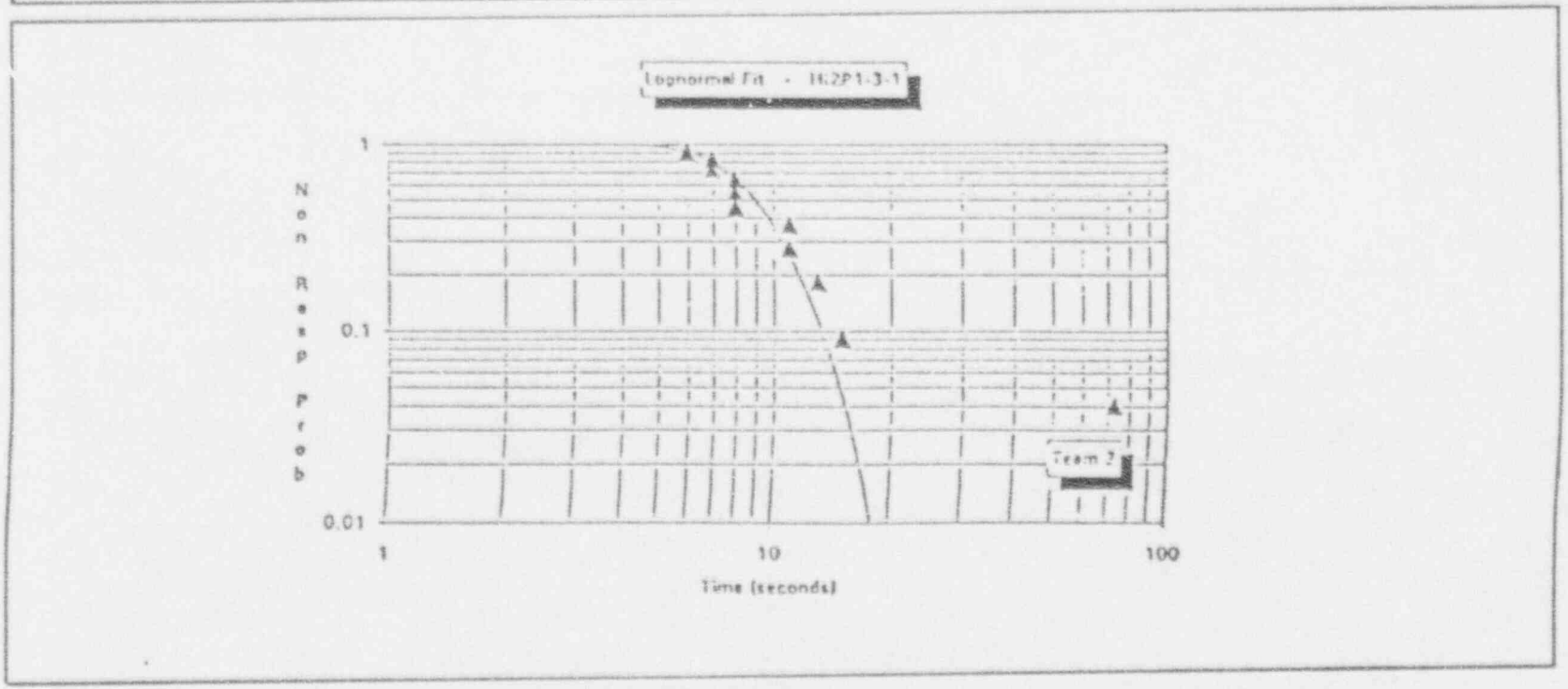

Figure 1. Normalized Time Matrix: Median Response Times for a Specific Human Interaction Illustrating Abnormal performance for One Team

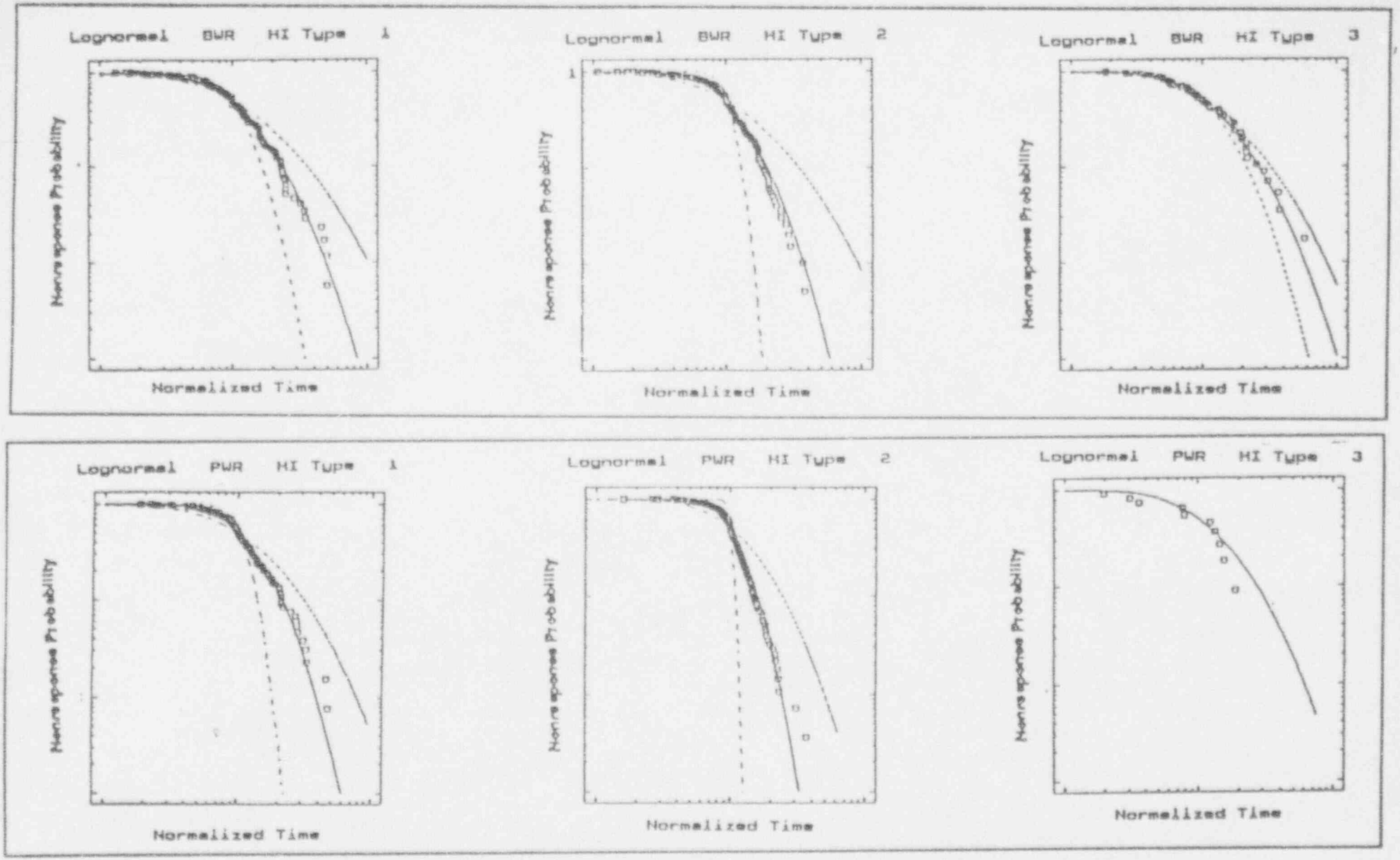

Figure 2. HCR/ORE Curves for Various Groups of Procedure-Based Human Interactions for BWRs (5% and 95% Uncertainty Bounds)

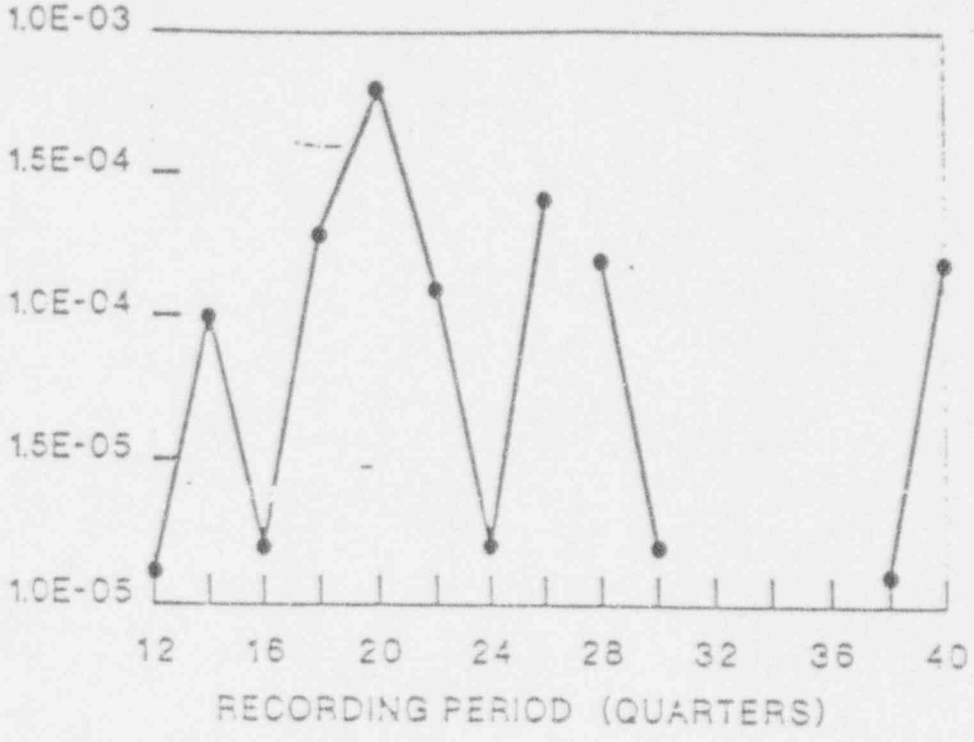

Figure 3. Core Damage Frequency Over Time

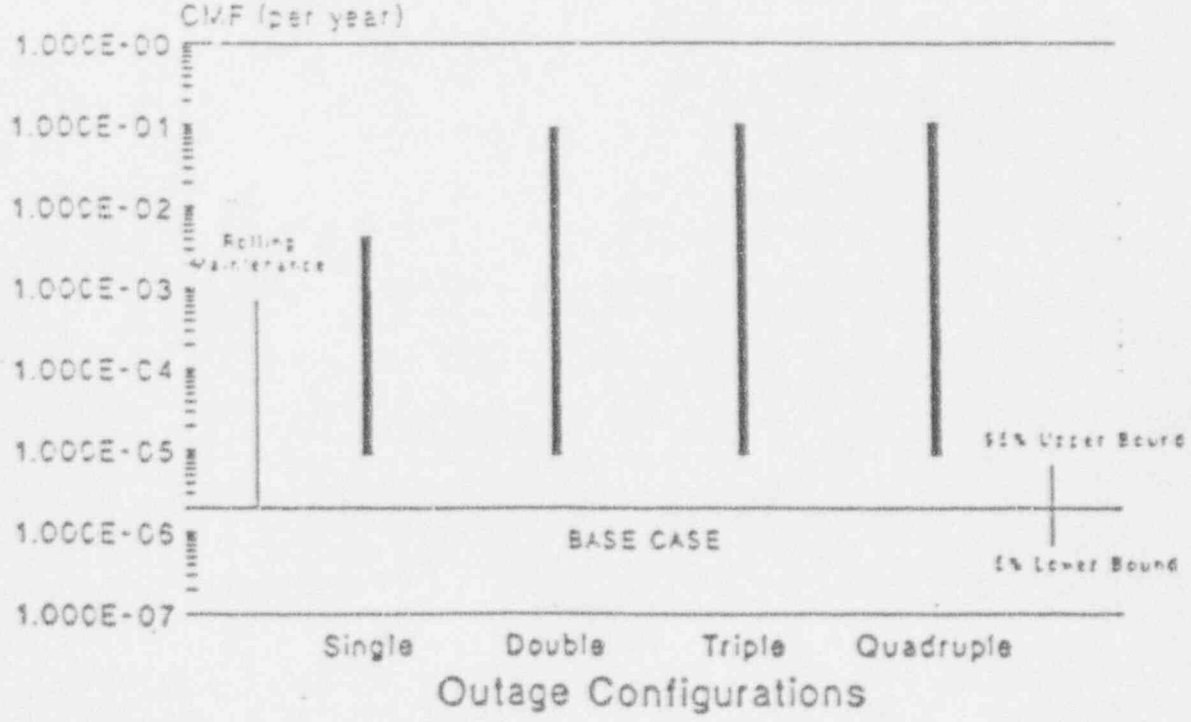

Figure 4. Range of CML Levels

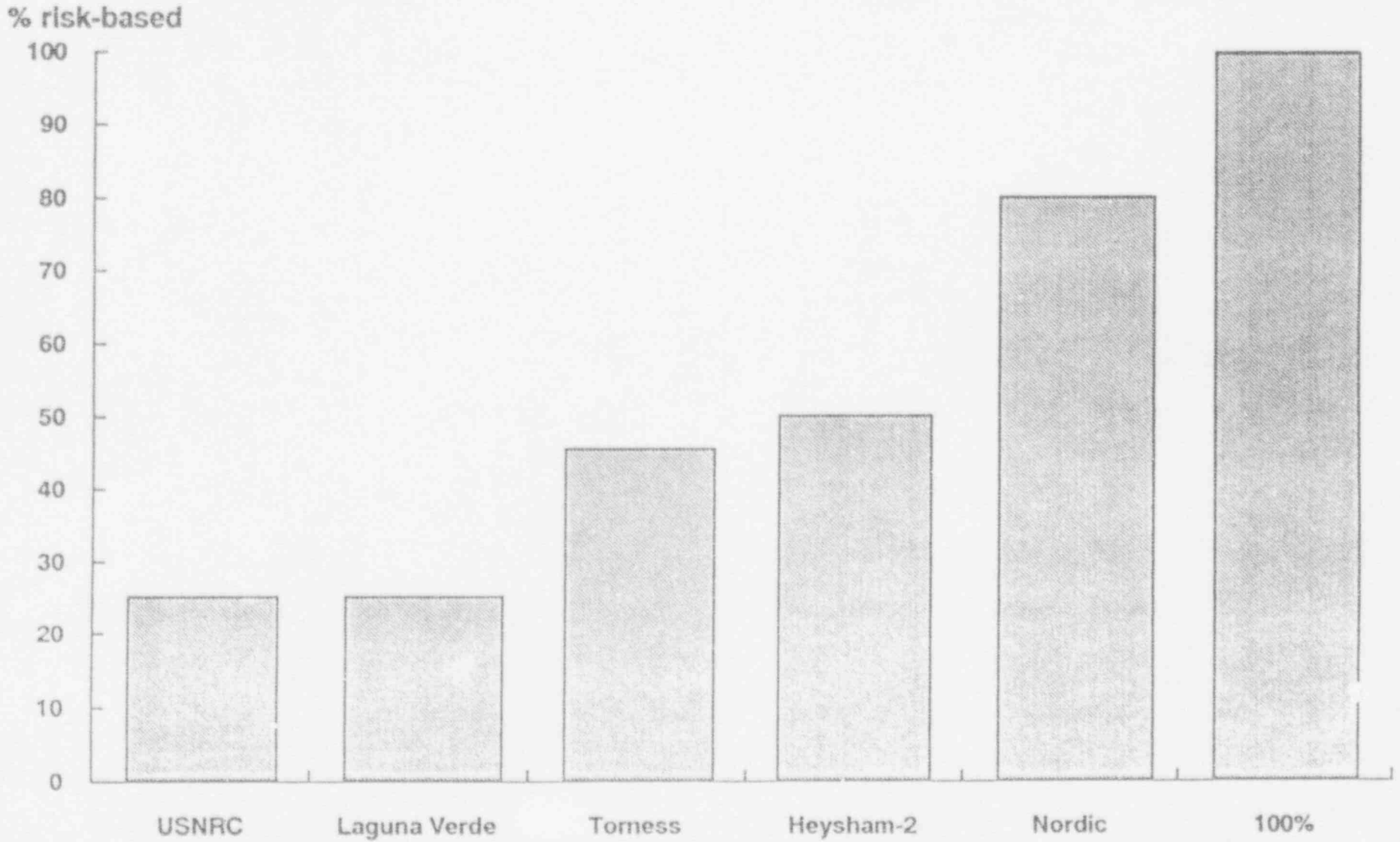

Figure 5. Risk-Based Usage in Regulation

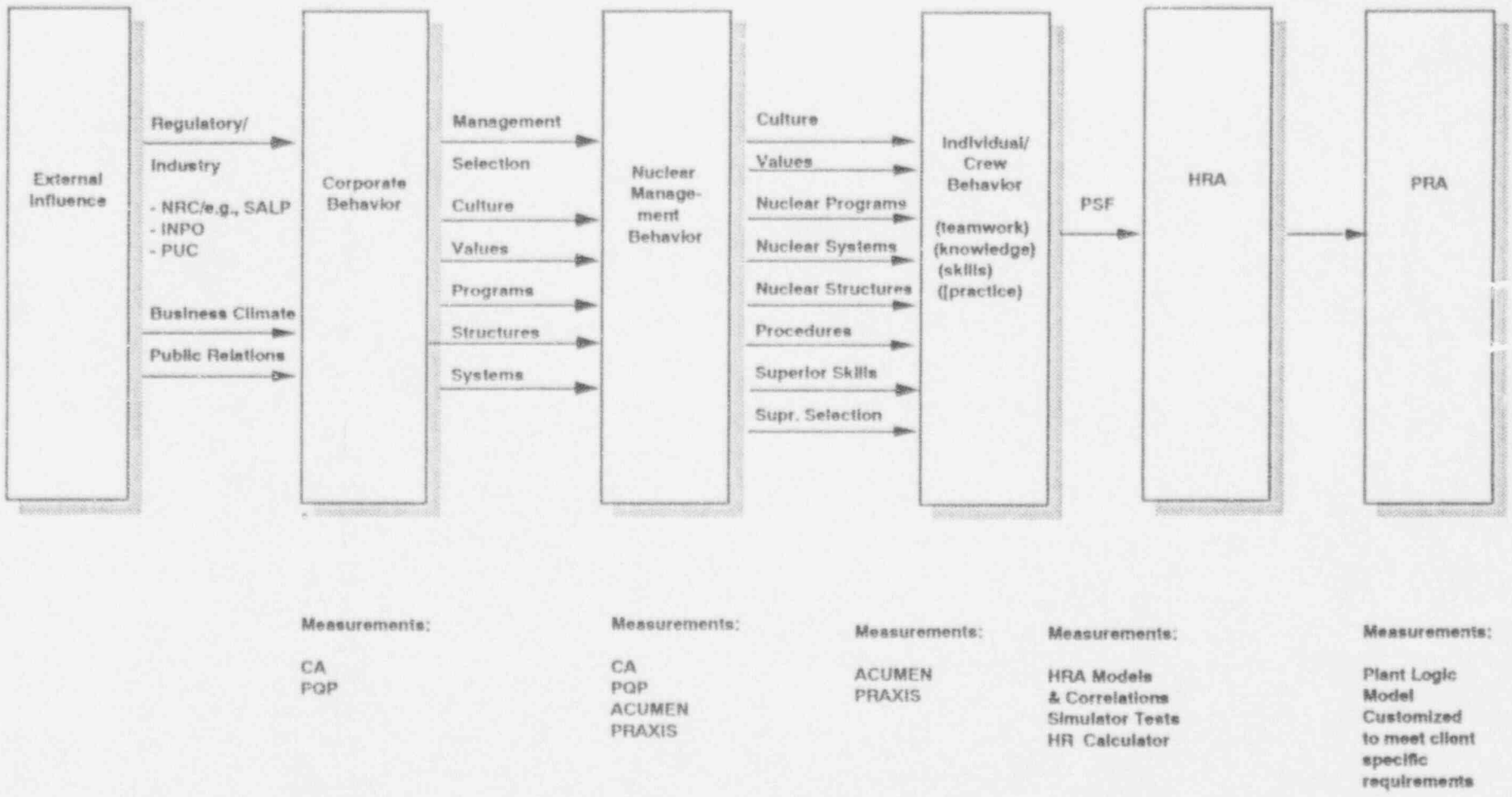

Figure 6. Integrated Risk Management Framework

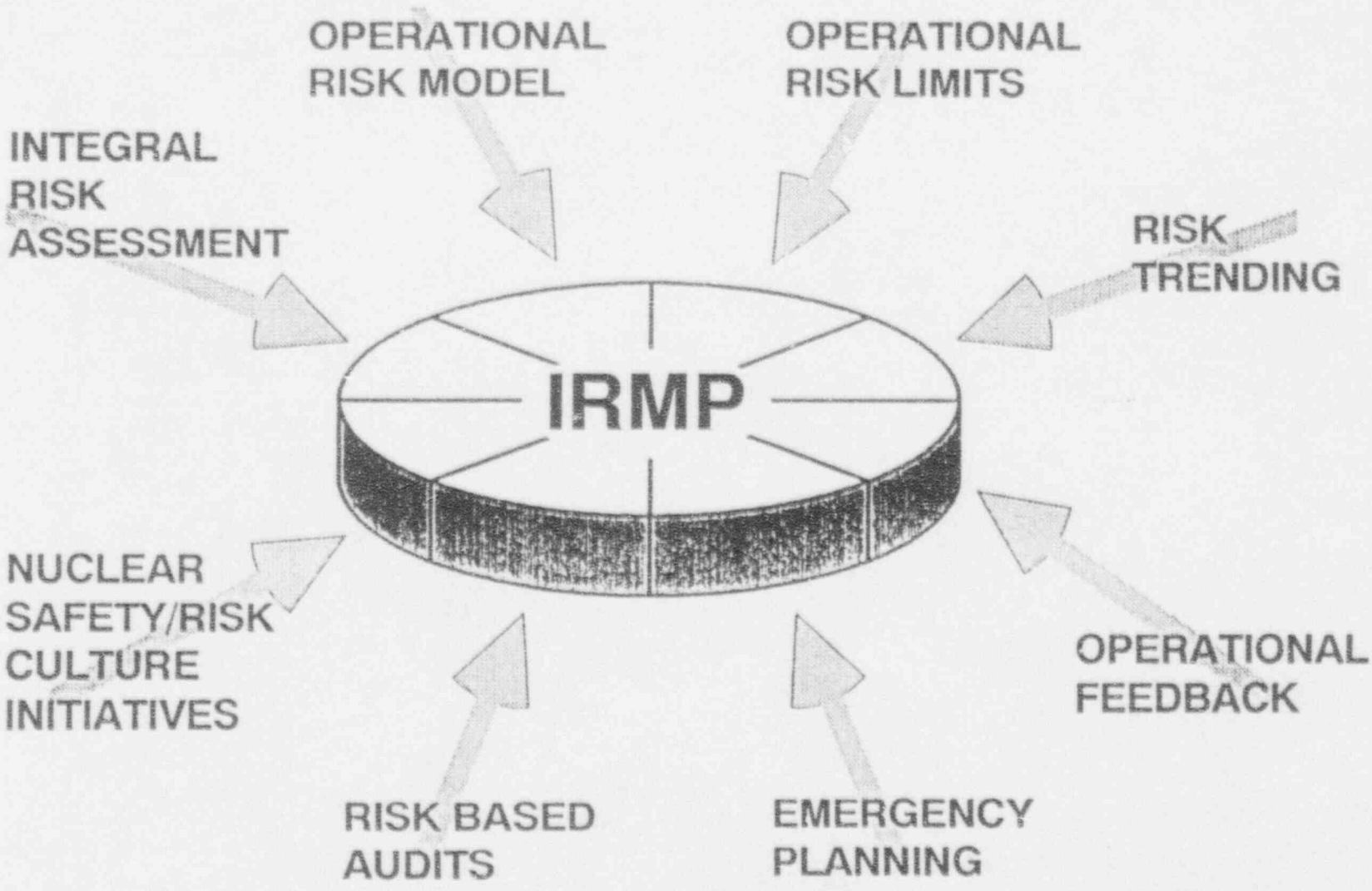

Figure 7. IRMP Principal Elements

Position	Knowledge															
	Risk Assessment			Details of the Plant			Transient Behavior			Severe Accident Management				Safety Basis		
	System Interactions	Human Factors	Dominant Contributors to Risk	Structures	Systems	Components	Reactor Physics	Thermal Hydraulics	Radionuclide Transport	Core Behavior	Vessel Integrity	Containment Capabilities	Mitigation Techniques	Design Basis	Technical Specs	Regulatory and Industry Standards
Management																
VP Nuclear Operations	1	2	2	1	1	1	1	2	2	1	1	2	2	2	1	2
Plant Manager	2	2	3	2	2	2	2	2	2	2	2	3	3	3	3	3
Operations Manager	3	3	3	2	3	2	2	3	2	2	3	3	2	2	3	2
Maintenance Manager	1	2	2	2	2	3		1	1	1	1	2	2	2	2	2
Technical Services Manager	3	2	3	2	3	2	2	2	2	3	3	3	3	3	3	3
System Engineers	3	2	3		3	2	2	3	2	1	1	1	2	3	3	2
Radiation Protection Engineers					1	1		1	3	2			2		2	3
Senior Reactor Operator	2	2	2	1	3	2	2	3	1	2	2	2	2	2	2	2
Labor																
Control Room Operator	2	1	1	1	2	2	2	2	1	1	1	1	1	1	2	1
Auxiliary Operator	1				1	1		1							1	
Instrument Tech Foreman	2	1			1	3	2	1	2	2			1	1	2	
Electrical Foreman	1	1			1	3							1		1	
Mechanical Foreman	1				1	3							1		1	
Radiation Protection Foreman					1	2			2				1		1	
Chemistry Technicians									2				1		1	

Figure 8. Knowledge Distribution Matrix

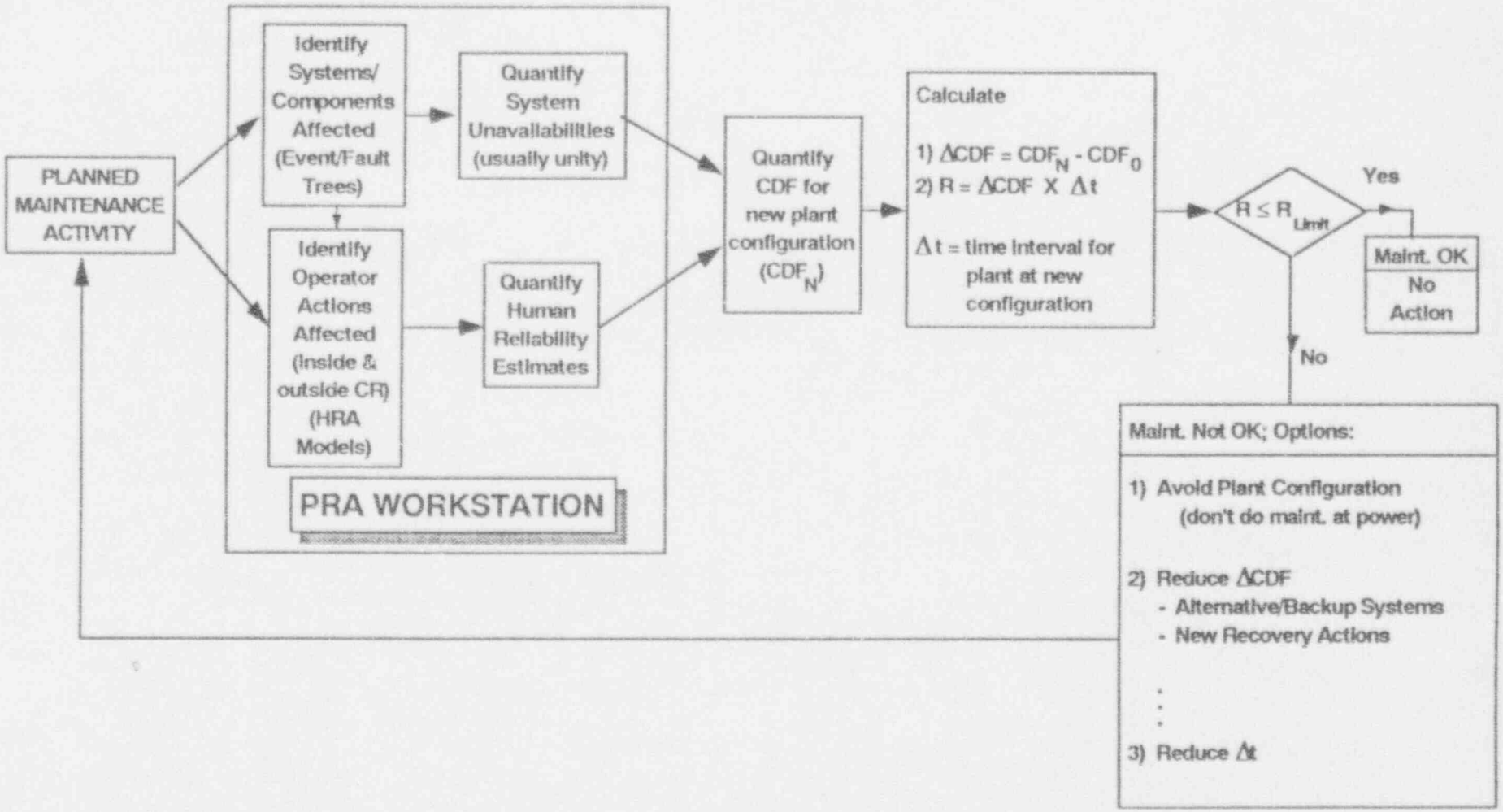

Figure 9. Risk-Based Maintenance Process Flowchart

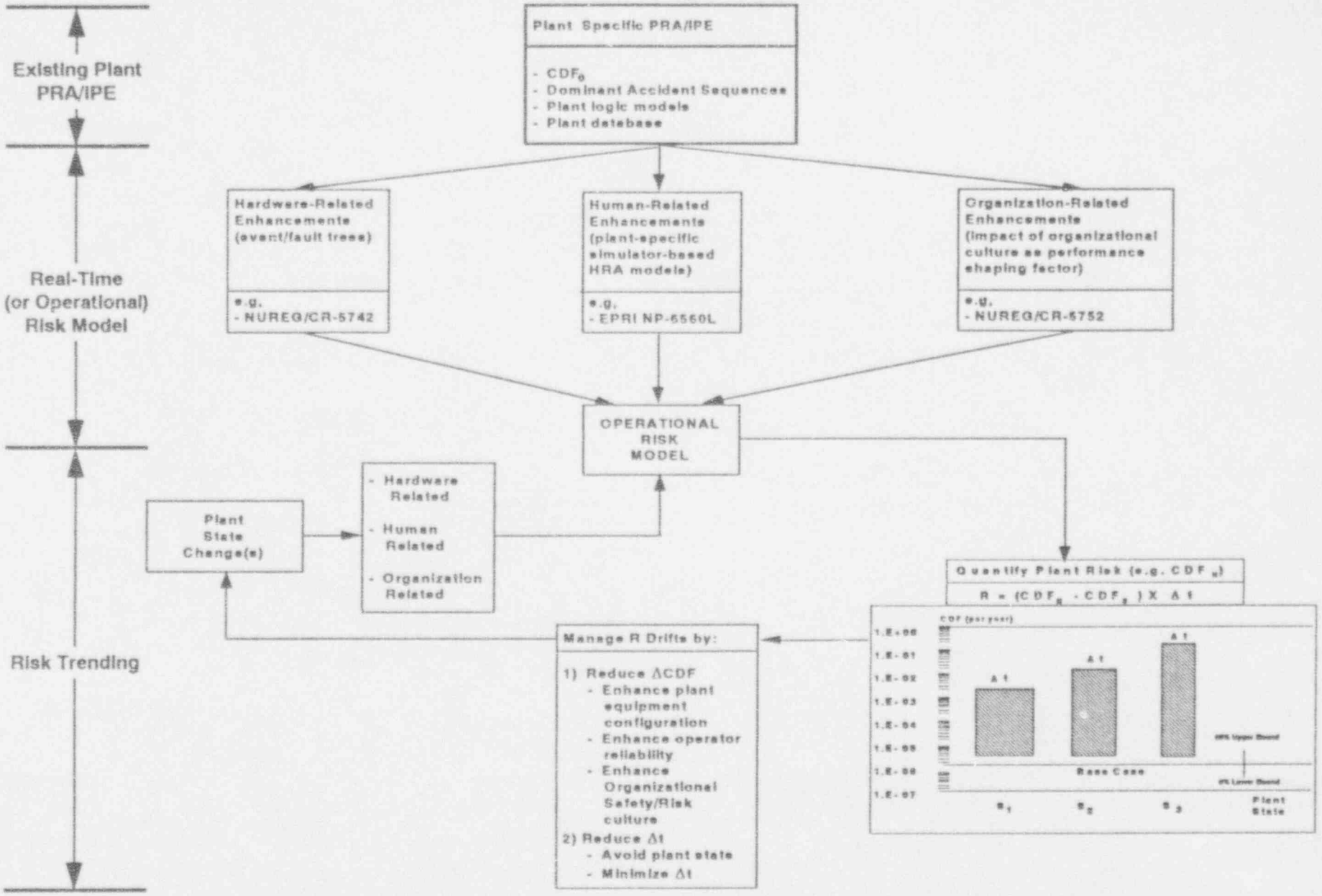

Figure 10. Operational Risk Management Flowchart

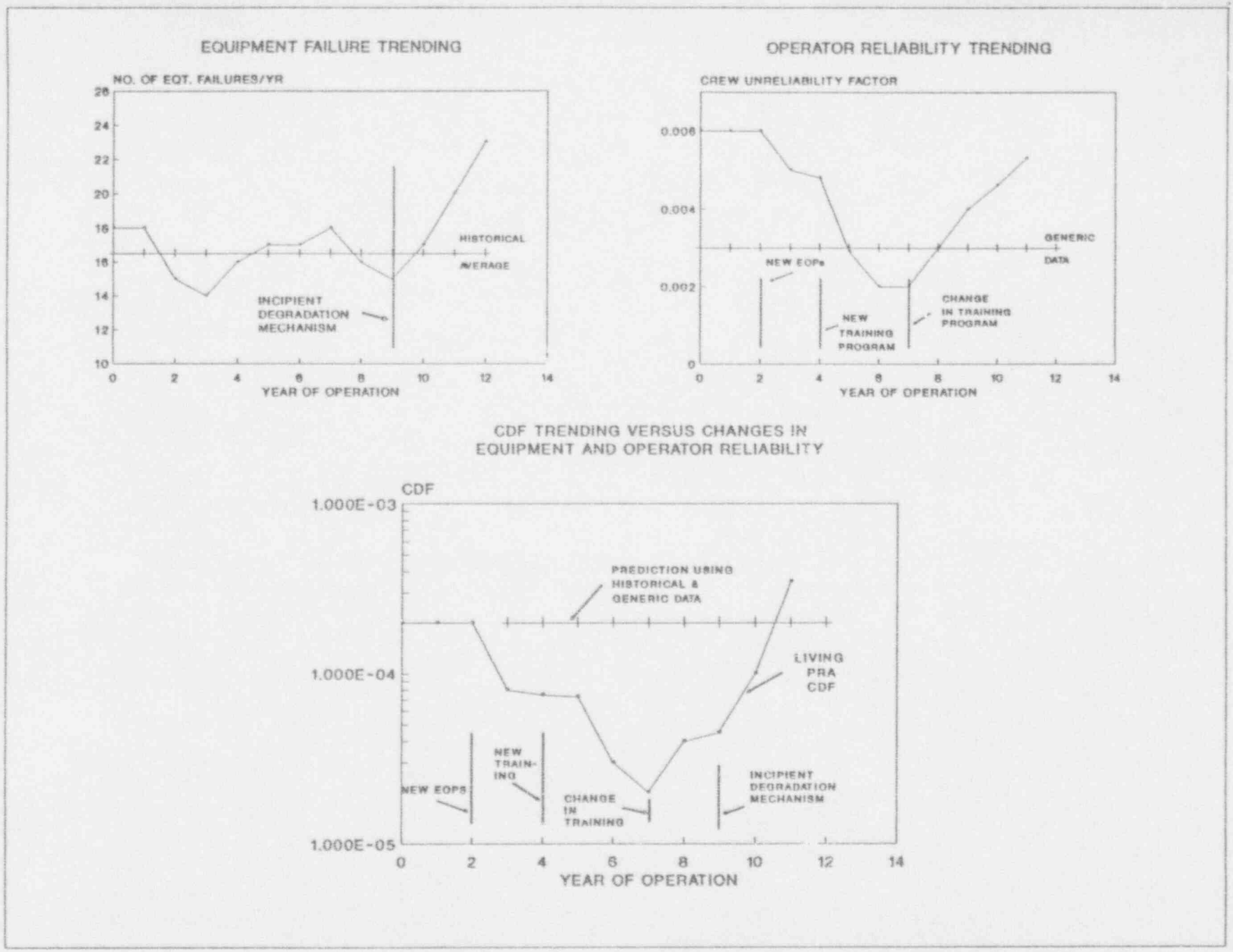

Figure 11. Schematic of Time Dependency of PRA and Risk Trending

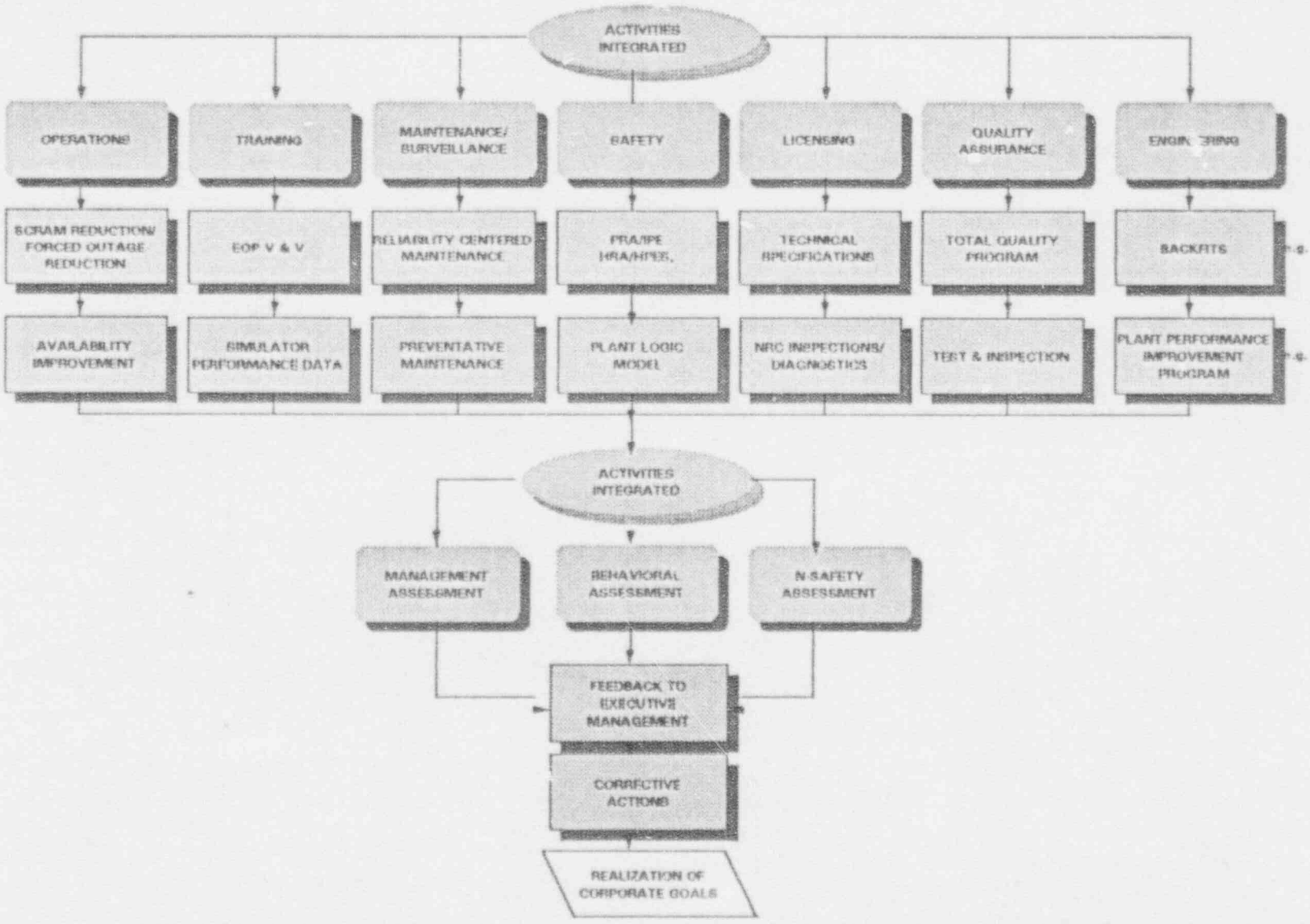

Figure 12. Organizational Units and Programs Important to NPP Safety

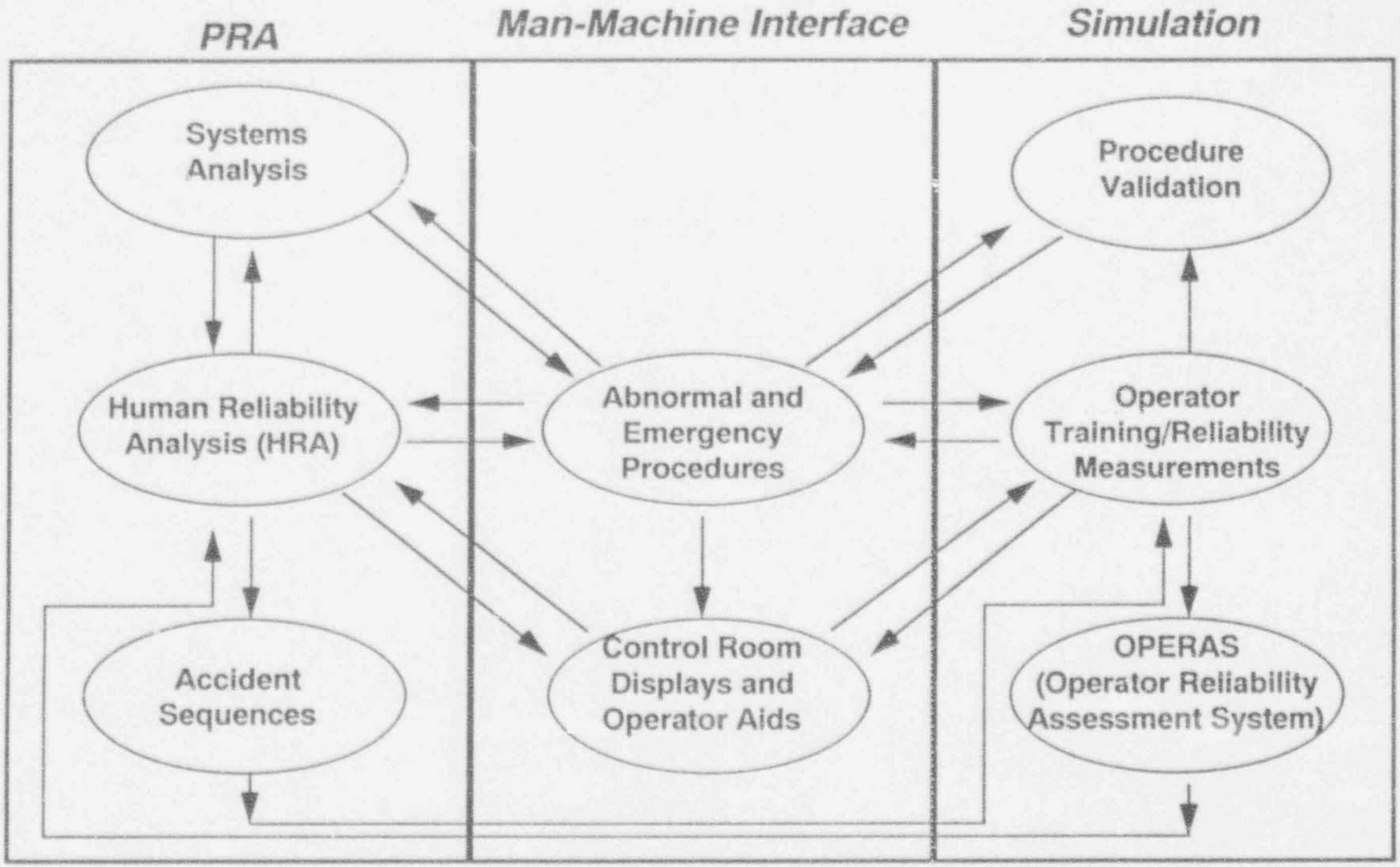

Figure 13. Human Reliability: Control Rool Activities

APPENDIX A: BIG ROCK POINT'S USE OF PRA IN LICENSING

Table 1

BRP ORIGINAL PRA EXEMPTION REQUESTS

Issue	Est Cost	Source*	Issue Status	PRA Method**
Plant Shielding	$40M	TMI	Exemption received	(1 and 4)
Post Accident Sampling	$300k	TMI	Exemption received	(4)
Instrumentation for detection of inadequate core cooling	$1M	TMI	Exemption expected	(1 thru 5)
Isolation of emergency condenser on high radiation	$50k	TMI	Exemption received	(1 thru 5)
Recirc loop interlocks	$50k	TMI	Exemption received	(1 thru 5)
TSC and Control Room habitability	$4M	TMI	Exemption received	(4)
Met tower and sirens	>$300k	TMI	Siren exemption denied Exemption given to scaled down met system	(4)

BRP PRA IDENTIFIED OR ENDORSED MODIFICATIONS

Early enclosure spray	$200k	PRA	Implemented	(1 thru 5)
PIR position locks	$10k	PRA	Implemented	(1 thru 5)
Remote FPS makeup to ECS	$25k	PRA	Implemented	(1 thru 5)
High pressure recycle procedure	$2k	PRA	Implemented	(1 thru 5)
PCS isolation valves	$25k	PRA	Refueling, 1985	(1 thru 5)
Feedwater instabilities	$25k	PRA	Refueling, 1985	(1 thru 5)
Alternate shutdown panel	$2.6M	APP R	Refueling, 1985	(1 thru 5)

*Key to Sources: PRC - Plant Review Committee; SEP - Systematic Evaluation Program; PRA - Probabilistic Risk Assessment; Gen Ltr - Generic Letter; TMI - TMI Action Plan; APP J-R - 10CFR50 Appendix

**PRA Methods used to develop technical arguments:

1. Logic model development
2. Sequence quantification
3. Plant and containment response
4. Consequence analysis
5. Cost-benefit analysis

Table 2

PRA EVALUATIONS PERFORMED SINCE 1981
Big Rock Point

Issue	Est Cost	Source*	Issue Status	PRA Method**
Shift staffing (need for SRO & STA)	$500k/yr	TMI	Exemption received	(1 and 2)
Recirc pump trip	$800k	Gen Ltr	Exemption received	(1 thru 3)
Diverse scram dump tank inst	$100k	Gen Ltr	Exemption received	(1 thru 3)
HELB inside containment	$1M	SEP	Exemption received	(1 thru 3)
HELB outside containment	$6k	SEP	Exemption expected	(1 thru 3)
PCS leakage detection	$100k	SEP	Under review by CPCo	(1 thru 3)
Thermal overload protection	$14k	SEP	Implemented (exemption expected to be denied)	
Main steam line isolation	$150k	SEP	Under review by CPCo	(1 thru 3)
Air lock testing	$60k	APP J	Exemption received	(1 thru 3)
Inst & service air auto isolation	$60k	SEP	Exemption expected	(1 thru 3)
Heating, cooling & service water auto isolation	$150k	SEP	Exemption received	(1 thru 3)
Treated waste auto isolation	$4k	SEP	To be implemented	
DC power monitoring	$50k	SEP	Exemption received	(1 thru 3)
Ventilation systems	UNK	SEP	Exemption received	(1 thru 3)
Interfacing LOCA	UNK	SEP	Exemption expected	(1 thru 3)
Electrical penetrations	$150k	SEP	Exemption expected	(2, 4 and 3)
Winds & tornadoes Tornado missiles	UNK	SEP	Under review by NRC	(1 thru 3)
Seismic design	>$2M	SEP	Under review by NRC	(1)
High point vents	>$10k	TMI	Exemption expected	(1 thru 3)
Scram dump tank LOCA	$25k	PRC	To be implemented	(1 thru 3)
Spurious RDS	$20k	PRC	To be implemented	(1 thru 3)
Turbine missiles	UNK	SEP	Exemption received	(2)
RHR htx tube failures	UNK	SEP	Exemption received	(1 and 2)
Hydrogen monitoring	UNK	TMI	Exemption received	(3)
Misc App R issues	UNK	APP R	Exemption received	(1 and 2)

APPENDIX B: ONE UTILITY SAFETY CULTURE INITIATIVES

PROCESS	PURPOSE	FOCUS	PERSONNEL INVOLVED	FORMATS
Teamwork & Leadership - Summer, 1986 - Present	Culture change, i.e., improvements in "the way we do things around here"	Improvement in "Core Values: (see pamphlet)	Internal facilitators and participants, mostly non-bargaining staff and line	Generic three day experimental sessions, plus various initiatives
• Risk Management-1987	Develop and implement a method for integrated risk management. Five year goal - 1990	Pilot a process for systematic, global, participative, identification, prioritization of risks in implementation of control measures - completed 1990		Generation of hazard scenarios and preventive actions which were then prioritized by line personnel
"Deming"-Summer, 1989, plus ongoing programs	Culture change, i.e., improvements in "the way we things around here:	Process improvements of various types - improve productivity by improving quality	Internal facilitators and participants, bargaining and management	Generic two day sessions, diagonal teams, follow-up sessions, use of statistics, etc.
• Organizational Culture and Nuclear Safety - 1989 and ongoing	Five year goal-1990	Phase 1 - Identification and measurement of variables Phase 2 - Define and implement appropriate actions for improvement	Plant staff	In process
• Attitude Survey - 1989 • Opinion Survey - 1992	Obtain employee views to improve effectiveness and make working more personally rewarding	Feedback from all employees	72% of company personnel	Questionnaire
Professionalism - 1990	Culture change, i.e., improvements in "the way we do things around here"	Consider dimensions of professionalism and illustrate the role of professionalism in efficient and safe operations of our nuclear plants	Internal facilitators and participants, bargaining and management	Two day participative sessions
• Policy Capturing - 1991	Improve decision-making with regard to risk	Discovery and explanation of decision-making value system of senior management	President's staff and Safety Review Board	Risk Management staff developed participant booklet to be completed and subsequently debriefed
Performance Improvement Program, 1992	Communicate purpose and management expectations	Two-way feedback	All employees	One-on-one session quarterly
Revised Nuclear Radiation Safety Plan, 1993	Communicate Senior Management policy and principles which predicated the plan	Nuclear and radiological safety responsibilities and accountabilities	All employees	Formal policy

APPENDIX C: RISK MANAGEMENT GUIDELINES (Large Scale Core Melt)

PERMANENT CMF INCREASE -OR-	ONE-TIME ORE MELT PROBABILITY INCREASE	CORPORATE RESPONSE	
		COMPENSATORY MEASURES	MINIMUM APPROVAL LEVEL
$<10^{-7}$/ YR	$<10^{-6}$	NONE	PRA SUPERVISOR
10^{-7} - 10^{-6}/ YR	10^{-6} - 10^{-5}	IF FEASIBLE	PRA SUPERVISOR
10^{-6} - 10^{-5}/ YR	10^{-5} - 10^{-4}	SERIOUS CONSIDERATION	V.P.
10^{-5} - 10^{-4}/ YR	10^{-4} - 10^{-3}	MANDATORY	SENIOR V.P.
$>10^{-4}$/ YR	$>10^{-3}$	UNACCEPTABLE	