Elsevier Science Publishers B.V., Amsterdam

Experience with probabilistic risk assessment in the nuclear power industry

J.S. Wu and G.E. Apostolakis

Mechanical, Aerospace and Nuclear Engineering Department, 38-137 Engineering IV, University of California, Los Angeles, CA 90024-1597 (USA)

(Received September 24, 1990; accepted in revised form February 15, 1991)

Abstract

Risk has become an important public concern for both nuclear and chemical industries over the years. In order to manage risk in a comprehensive and quantitative manner, the nuclear industry has developed the probabilistic risk assessment (PRA) approach over the past two decades. The chemical industry, on the other hand, has just started its efforts toward the quantification of risk. This paper presents an overview of the experience learned from PRAs for nuclear power plants. It gives a brief historical perspective of the development of PRA in the nuclear industry and reviews the methodology used in most current PRAs. In addition to the discussion of lessons learned, this paper also discusses issues related to PRA methodology that are still under development. Finally, some comments are made on the possibility of use of PRA in the chemical industry.

1. Introduction

The application of risk assessment to engineering can be traced as far back as the nineteenth century, when boiler codes were developed by mechanical engineers based on results of a qualitative and semi-quantitative risk assessment in an effort to reduce the frequency and consequence of boiler-related accidents. The current large scale quantitative risk assessments conducted for major industries, however, have evolved from *Reactor Safety Study* (RSS) [1] (otherwise referred to as WASH-1400), in which the risks from nuclear power plants were examined in terms of both severity and likelihood. Although there is continual improvement of its models, today's probabilistic risk assessment (PRA) approach, used widely by nuclear industry, is fundamentally based on the framework developed by the RSS. Note that when safety rather than risk is emphasized, as preferred by some utilities and also by the International Atomic Energy Agency (IAEA), the term 'probabilistic safety assessment' (PSA) is used in the place of PRA.

Correspondence to: Dr. G.E. Apostolakis, Mechanical, Aerospace and Nuclear Engineering Department, 38-137 Engineering IV, University of California, Los Angeles, CA 90024-1597 (USA)

0304-3894/92/$05.00 © 1992 Elsevier Science Publishers B.V. All rights reserved

This paper presents an overview of the experience gained from PRAs for nuclear power plants. Section 2 gives a brief historical perspective of the development of PRA in the nuclear industry. Section 3 reviews the methodology used in most current PRAs, and Section 4 discusses lessons learned by the United States Nuclear Regulatory Commission (USNRC) and the nuclear industry from the experience of past PRAs. In Section 5, the on-going issues related to PRA methodologies that are still under research are discussed. Finally, Section 6 offers some observations on industry-specific applications of PRA. Although this article has a broad view of the developments and applications of PRA, the discussion is dominated by the US experience, since it is closer to the author's experience.

2. Historical perspective

The first major study to address reactor safety issues was WASH-740 more than 30 years ago [2]. This study was done with limited information and resorted to the estimation of rough upper bounds for the consequences from a large release of radioactivity. While the authors of that report cautioned its readers not to appraise their conservative results independently of their probabilities, many readers nevertheless became very concerned about the hypothetical consequences reported.

Farmer's paper in 1967 [3] described a "new approach" that was based on the premise that the risk from a system was better represented by the probability of system failures and their consequences. He proposed his now famous Farmer's line that defined "acceptable" from "unacceptable" releases. His concept of risk as a two-dimensional measure—probability and consequence—has had a significant impact on the latter on risk assessments.

In the United States, the history of the application of PRA shows a change in the attitude of both the USNRC and the nuclear industry. *Reactor Safety Study* (1975) took Farmer's concept of risk and focused on events that had the potential of leading to core damage and subsequent radiological impact on public health and safety. Its results, presented in curves of consequences and their corresponding likelihoods, conveyed the message that the risks from nuclear reactors were very small compared with other risks (natural and man-made) that already exist. Although widely discussed, the safety-related insights and PRA techniques developed by the RSS were largely ignored by both the USNRC and much of the nuclear industry for years. Opponents of nuclear power immediately launched political and technical attacks on the credibility of the report and eventually achieved considerable success in discrediting the report.

In response to this criticism, the Risk Assessment Review Group [4] undertook the task of reviewing the RSS. This report, commonly referred to as the Lewis Report, criticized selected areas of *Reactor Safety Study,* but strongly supported the overall approach and suggested further use of the methodology in the regulatory process. The policy statement [5] issued by USNRC in January 1979 in response to the Risk Assessment Review Group report, however, took a position directly opposite to the recommendation made in the report. The USNRC's negative attitude was a major setback to the development and application of PRA.

The accident at the Three Mile Island (TMI) nuclear power plant in March of 1979 changed the USNRC's attitude towards the development and application of PRA. The fact that the TMI accident was beyond the conventional design basis accident and that the RSS had analyzed similar event sequences prompted both the USNRC and the nuclear industry to reevaluate the merits of PRA. The subsequent reports by the President's Commission on the accident at Three Mile Island [6] and by the USNRC's Special Inquiry Group [7] contained strong endorsement of PRA techniques. Since then PRA has been widely accepted by the nuclear community in the United States as a valuable tool for providing measures and insights to reactor safety.

Several milestones marked the development of PRA within the USNRC through the 1980s. General procedures for performing PRAs were published in 1983 [8] in response to the need for technical guidance in performing PRA. This was followed by a summary of PRA insights available in the early 1980s [9], in which detailed discussions from the USNRC's standpoint were given on several aspects: the development of PRA, its strengths and uncertainties, insights drawn from the PRA studies performed to that date, the possible application of PRA to the regulation of nuclear power plants, and related difficulties. Later on, the USNRC developed the Source Term code package [10] containing a new computational model for severe accident physical processes and providing a more sophisticated view of the consequence end the PRA methodology. The USNRC also issued policy guidance on how severe accident risks were to be assessed [11] and policy guidance on safety goals against which these risks could be compared [12].

In 1988, the USNRC issued a generic letter in which each licensed nuclear power plant was asked to perform an "individual plant examination" (IPE), which would provide information on the assessment of severe accident vulnerabilities. According to the IPE letter, each plant would have the option to perform such examination via PRA or other approved means. The purposes of the IPE are to identify the vulnerabilities of each plant during severe accidents and to enhance plant safety by designing safety strategies to account for these accidents. The most recent major PRA-related effort sponsored by the USNRC is the NUREG-1150 study [13], which utilizes technologies developed through the 1980s to provide "a snapshot (in time) or estimated plant risks in 1988" at five commercial nuclear power plants of different designs.

Starting in the early 1980s, utilities in the United States have gradually appreciated the quantitative insights of PRA, especially in keeping operational and engineering personnel better informed. A utility PRA team typically consists of PRA specialists and system engineers from the consulting firms, the reactor vendor, the architect–engineer, and the utility itself. The first two such studies that were released after the accident at Three Mile Island were the Zion probabilistic safety assessments (PSA) of 1981 [14] and the Indian Point PSA of 1982 [15]. After these two studies, more than 30 large scale PRAs sponsored by utilities were completed in the 1980s. With the issuance of the generic letter on IPE by the USNRC in 1988, it is expected that more utilities will expand their PRA capability and application in the coming years.

Outside the United States there has been a similar history. The German Risk Study [16], published in English in 1981, essentially applies the RSS methodology to the reference nuclear power plant Biblis B sited in the Federal Republic of Germany. In the United Kingdom, PRA methodology has been applied to Sizewell, B, a nuclear power plant in its design stage, where plant safety is expected to be improved from PRA insights gained in the early stage of plant design [17]. Other countries have also performed similar studies.

3. Overview of PRA methodology

Unlike the chemical process industry, in which various inventories of hazardous chemicals present different degrees of threats located throughout its plants, the nuclear industry has the unique feature of a single primary hazard location at its plant, i.e. the nuclear reactor core where its radioactive material inventory concentrates. The major concern for the safety of the nuclear power plant is, therefore, how an accident that may lead to reactor core damage could occur, and how likely it would be; furthermore, if reactor core damage occurred, how much and how likely would the radioactive material inventory be released into the atmosphere. Finally, how much threat such a release would impose to the public health.

The PRA methodology has been developed so that the safety and operational characteristics of complex technological systems can be investigated systematically. The methodology considers two important features of large and complex systems:

1. The consequences of major accidents are potentially very severe, and thus, their occurrence is a matter of public attention and concern.
2. These major accidents are rare events, and any related decision-making process must include the large uncertainties that are associated with their occurrence.

The PRA methodology thus developed has focused on these two core issues. Specifically, it consists the following two steps:

(1) The identification of scenarios (accident sequences) that have the potential of leading to undesired consequences, such as system unavailability, the release of radionuclides, and so forth.

(2) The quantification of the uncertainty associated with the occurrence of these scenarios.

The identification of the scenarios follows the logic depicted in Fig. 1 [18]. The process begins with the selection of a set of initiating events (IE), i.e. events that have the potential to start an accident scenario. Initiating events, in general, fall into one of the following two categories: internal and external events. Internal events are those events that may occur due to abnormal operation of the system. For example, the internal initiating event "loss of coolant accidents" (LOCA) generally refers to events involving breaks of coolant pipes of various sizes. This leads to the loss of water from the reactor vessel and subsequently causes a reactor trip. External events, on the other hand, are events occurring externally to the system. Earthquakes, fires and tornadoes are examples of external events in PRAs. External events often have an impact on more than one component or system. For example, two or more components may fail simultaneously during an earthquake if the intensity of the earthquake is much higher than the designed capacity of the components. For a more complete discussions of initiating events, refer to earlier work [8,19,20].

In the process of identifying accident scenarios, the possible responses of the plant to the occurrence of an initiating event are modeled by employing event trees. Each branch point of the event tree represents the possibility that the corresponding safety system (or function) may or may not be available. For branches that involve failures of safety functions, the failure modes of the safety systems are defined and fault tree analysis [21,22] is employed to find possible combinations of component failures and/or human errors that might lead to these failures. The paths in the event trees define the accident sequences. Each of these sequences leads to a "plant state", i.e. a particular state of the nuclear reactor that defines a set of initiating and boundary conditions for later analysis. Any PRAs completed up to this point are called "Level 1" PRAs [8].

Given damage to the reactor core, as specified by the plant states, the analyst may wish to continue to develop the accident scenarios by following the progression of physical phenomena after the core has been damaged. This enters the scope of Level 2 PRAs, of which the end points are the various release categories of radioactivity to the environment. Level 2 PRAs include the analysis of physical processes and of fission product transport. In the physical process analysis, the variation of temperature and pressure inside the containment building and its possible failure modes are investigated. The fission

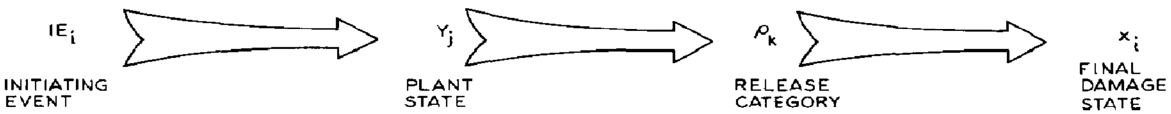

Fig. 1. Overview of the process for nuclear plant risk analysis [18].

product transport analysis determines the amount and timing of radionuclide releases into the atmosphere.

If the accident sequences are analyzed further to include the site characteristics related to public health and safety, then the PRA is said to be at "Level 3". Level 3 PRAs, in general, include three types of analysis: dispersion analysis, in which radionuclides are dispersed and carried by the plume of gases released from the containment or otherwise transported by some pathway through the environment to man; dosimetry analysis, in which exposure of human organs to radiation is calculated; and consequence analysis, in which the conversion is made from exposure to human health effects.

While different methods are employed to various degrees of sophistication in quantifying the risk, the rigorous and formal methods of Bayesian or subjectivistic probability theory [23,24] are gaining increasing acceptance. Probability in the Bayesian framework is interpreted as a measure of the degree of belief in accordance with De Finetti [25]. Admissible evidence consists not only of the conventional statistical type, but also includes expert judgment stemming from knowledge of the process and operational experience. The use of expert opinion is necessary in PRA, both in modeling and in quantification, because the events of interest are rare and statistical evidence is either very weak or non-existent. This extensive use of judgment often creates conflicts between parties of opposite stake-holders. While formal methods, such as the Bayesian approach, help in understanding the differences, they are nevertheless unable to resolve all the issues that arise in the elicitation and use of judgment. Although non-probabilistic interpretation of uncertainty has gained some ground in recent years, it has not reached a state of development that can be used in quantifying risk. Some discussion of the probabilistic and non-probabilistic interpretation of uncertainty can be found in [26,27]. Further discussion on the Bayesian approach used in PRAs can be found in [28,29].

4. Experiences of PRA

4.1 General perspective

Over 30 PRAs have now been completed in the United States and other countries. While most results are plant-specific, the PRAs performed to date have reached some general conclusions that are useful in helping the nuclear regulatory authorities and the nuclear industry to understand the general features of nuclear power plant safety.

4.4.1 Frequencies of core melt

The PRAs performed to date on nuclear power plants show that core melt frequencies range from 10^{-6} to 10^{-3} per reactor year. Aside from plant-to-plant variation, a good part of this wide range is due to the difference in modeling and the variation of scope in various studies. These core damage frequencies are greater than the numbers that the industry had generally believed possible prior to the development of PRA methodology. This over-confidence prior to the PRA era can be attributed to two safety concepts that the earlier reactor designers had strongly relied on:

1. It was believed that the reactor would be safe if it were designed for the worst credible accident.
2. Redundancy in safety-related components would greatly reduce the chance of accidents.

The first concept evolved into the concept of the design basis accident (DBA) [30], in which accidents following large pipe ruptures were defined as the DBA against which the emergency core coolant system (ECCS) should be designed. The second concept led to the single failure and separation criteria that were used in the design of safety systems. The design criteria based on these concepts have been traditionally called "deterministic design criteria". What the deterministic design criteria failed to demonstrate in the past, and PRA has successfully shown over the last two decades, is that accidents other than DBA contribute significantly to the core melt frequencies, which runs against the beliefs held by the earlier designers. This is shown in Fig. 2 [31]. The results of Level 2 and Level 3 PRAs also indicate that certain rare accidents beyond DBA could dominate "risks" (a loose index for plant risk determined by probability×consequences) even if these sequences are not necessarily dominant in core melt frequencies. Furthermore, the common cause failure issues raised in the PRA community have pointed out that redundancy does not improve the system reliability to the degree that the reactor designers used to believe [32].

A less surprising observation was made in the studies that surveyed "external" events, namely, earthquakes, fire, flooding, aircraft crashes, etc. Figures 3 and 4 [33] show that the fraction of core melt frequencies resulting from external events varies significantly from plant to plant. This variation is largely due to the fact that these plants, although sharing the same general design and operating characteristics, are quite different in geological siting and other aspects. The large uncertainty in both data and modeling in the analysis of external events also contributes to this variation in fraction of core melt frequencies.

4.1.2 Containment performance and severe accident source terms

All major studies [1,10,13] have confirmed that the consequences of severe reactor accident depend greatly on the safety features of the reactor containment and its ability to retain radioactive material. Figure 5 [31], for example, displays the results of several studies for iodine releases. As shown in the figure, the largest fraction of core inventory released to the environment comes from accident sequences that lead to early containment failure of containment bypass. The release fractions are less for sequences that lead to late contain-

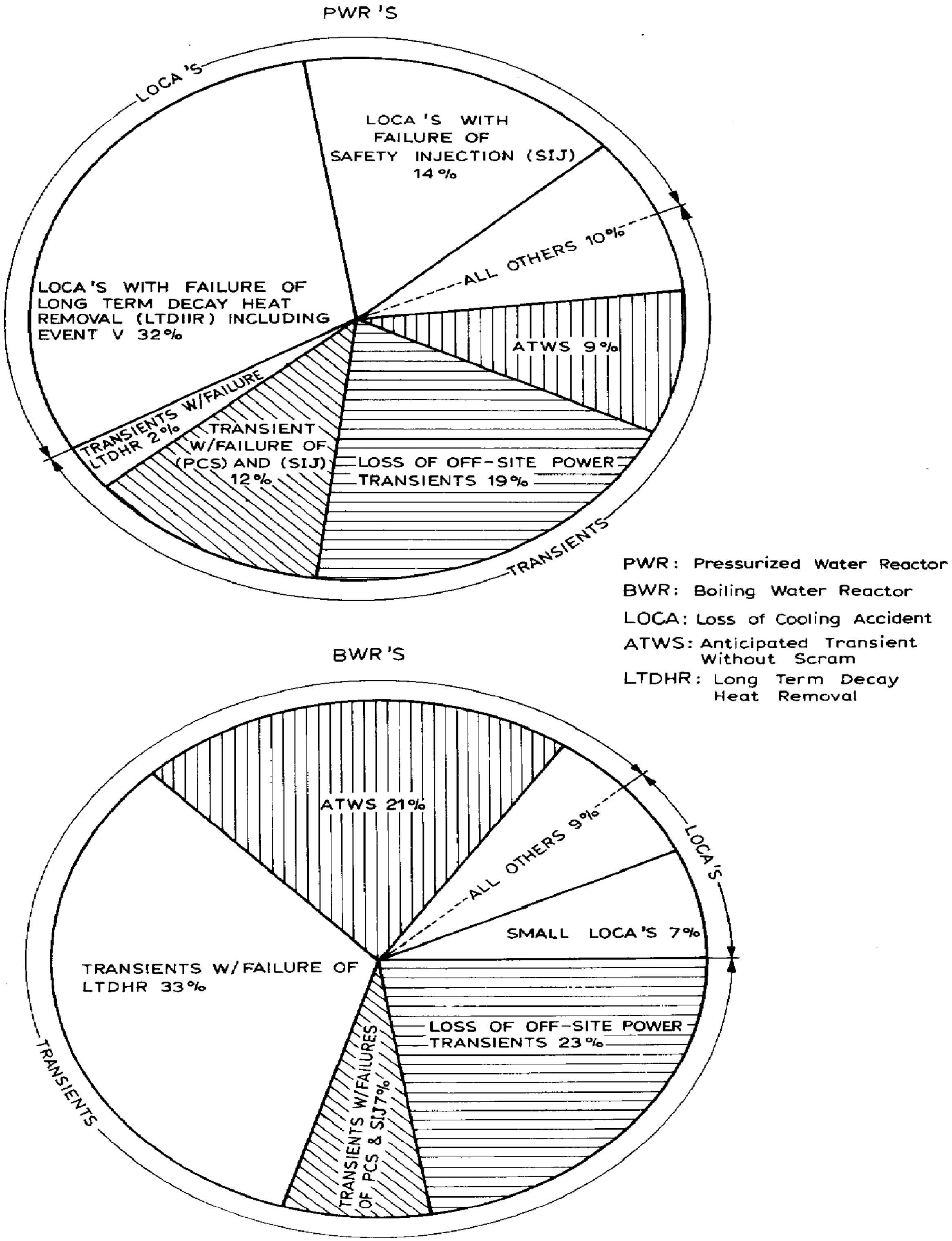

Fig. 2. Composite of major contributors to core melt frequency [31].

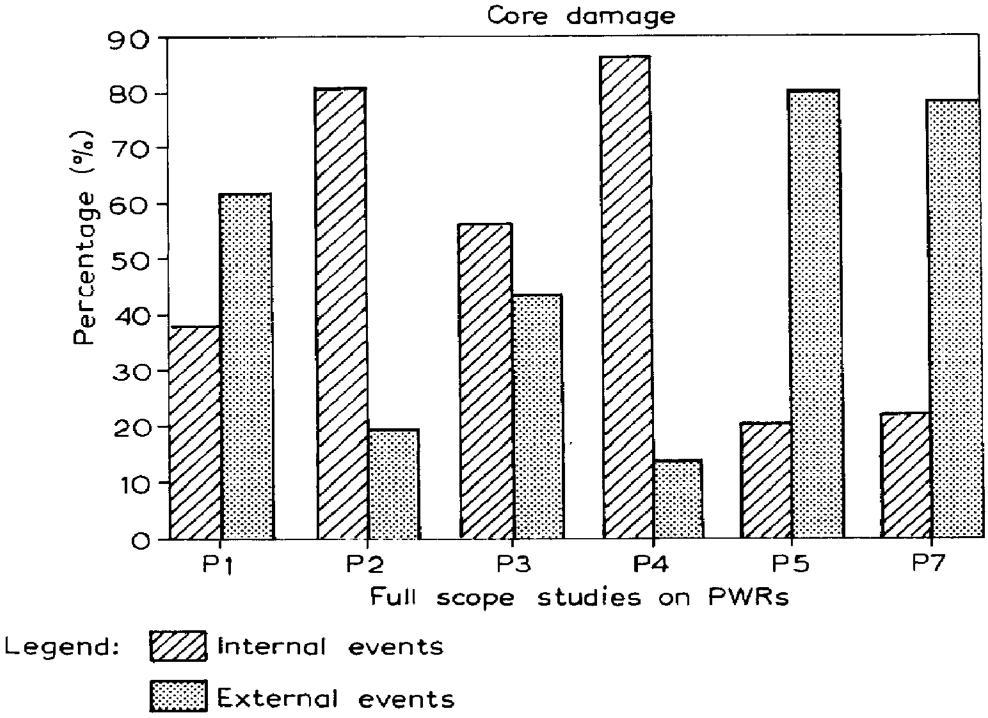

Fig. 3. Internal versus external contributors to core damage [33].

ment failure or no containment failure. This trend can be explained by the fact that the longer the containment remains intact—i.e. the time interval between core melt and fission product release from the reactor coolant system—the longer the radioactive material can be removed from the containment atmosphere via engineered safety features or natural deposition processes; thus, a smaller fraction of radionuclide inventory is released to the environment.

4.1.3 Public risk

One of the primary objectives of the PRA studies is to obtain insights regarding the risk to public health from severe accidents at nuclear power plants. The frequency of events with severe off-site consequences are generally found to be very low for nuclear power plants. Using expected early fatality rates and latent cancer rates as risk indicators, the *Reactor Safety Study* concluded that risks from nuclear plants are relatively lower than risks from other man-made and natural hazards [1]. The more recent NUREG-1150 study [13] indicates that the risk (in terms of probability × consequences) to the public from operation of the five plants studied are, in general, even lower than those of the *Reactor Safety Study*, and the estimated public risk is within the safety goals that have been proposed by the USNRC [12].

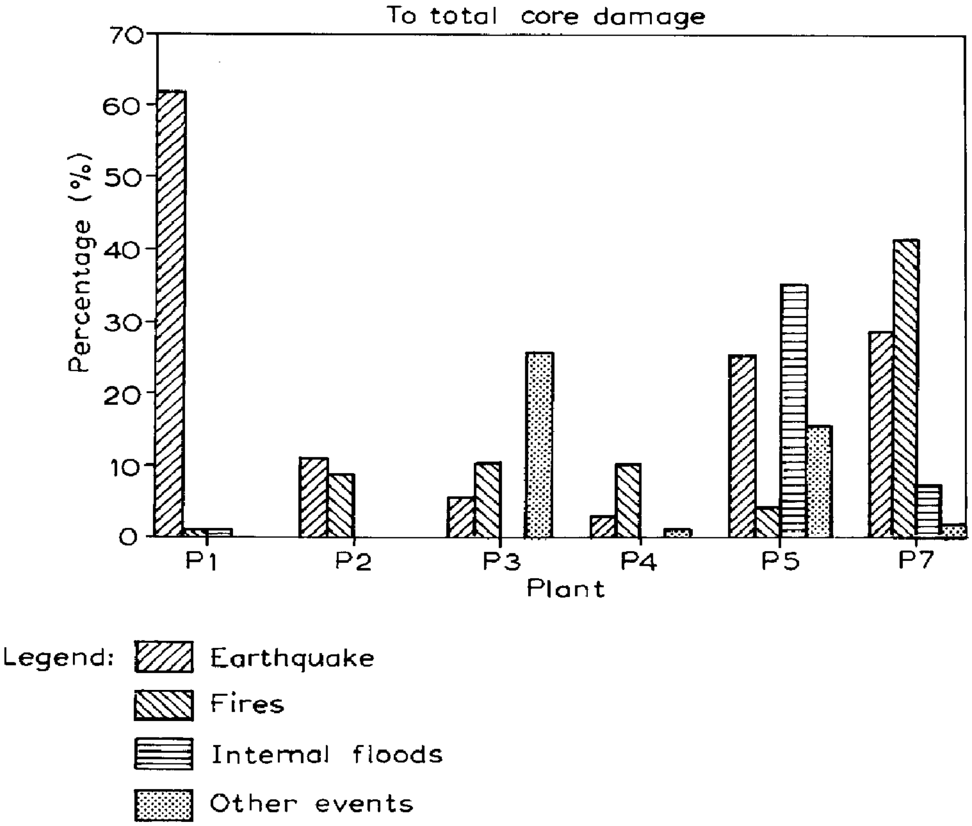

Fig. 4. Contribution of external events [33].

These low frequency high consequence events have long been a problematic issue for a nuclear regulatory and decision-making body. In some countries, special measures have been taken to mitigate or render still more improbable these rare accidents, e.g. by introducing filtered-vent equipments, although simplistic cost–benefit analyses based solely on expectation values could indicate these measures to be clearly not cost effective.

4.2 The role of PRA in the nuclear regulatory process

Probabilistic risk assessment, which provides a logical way of examining reactor safety, has evolved from normal design practices and the regulatory process. Under this approach, the traditional safety philosophy used in the nuclear regulatory system, which included single-failure and separation criteria, DBAs and the sometimes thought-to-be conservative attitudes, has not always effectively safeguarded the safety of nuclear power plants [34,35]. The TMI-Unit 2 accident amplified such worries. Since then, the USNRC has in-

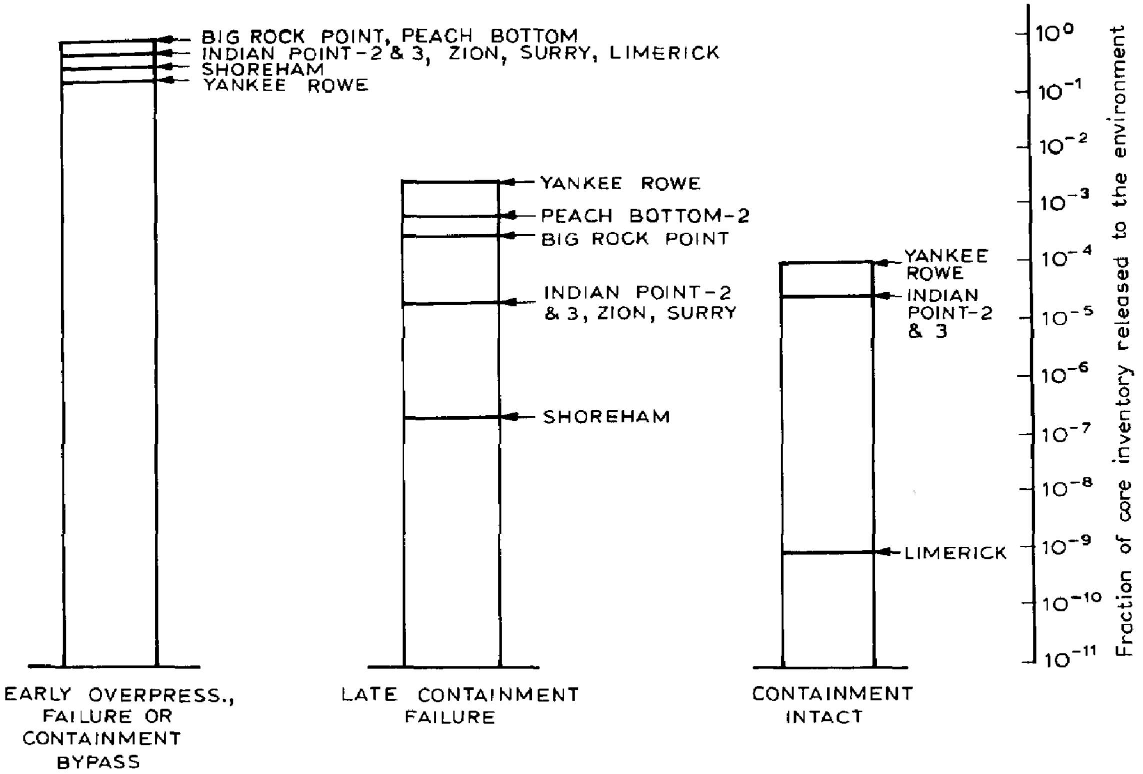

Fig. 5. Iodine release fractions from listed PRA studies [31].

creasingly used PRA techniques in various aspects of the regulatory process. In the following discussion, we address two regulatory uses of PRA within the USNRC.

4.2.1 Allocation of regulatory resources [9,36]

One of the regulatory applications of PRA is to set priorities for regulatory resources in resolving generic safety issues [37]. These safety issues are identified by the USNRC, based on experience or analysis at specific plants, as issues that may raise safety concerns over an entire group of plants. For example, the USNRC may raise safety issues concerning reactors of the same nuclear steam supply system (NSSS) vendor that are similar in design and operation. Since the analyses that the regulatory decisions are based upon do not require great precision, often analyses with broad categories of risk impact (e.g. high, medium and low) would provide enough information for setting priorities of this type. A potential safety issue would only be dismissed, if it were clearly of low risk. Information and insight from PRAs can be used as bases for assigning risk impacts and determining the general direction of regulatory priorities, even though they do not fully represent the characteristics of all plants.

Other than allocating resources on generic safety issues, information from PRAs can also be used to guide the allocation of resources in inspection and safety enforcement programs. Items identified by PRA studies to be significant to the safety performance of the plant will be assigned higher priorities in the implementation of quality and reliability assurance programs. The PRA results also provide a means in assigning priorities for auditing component and system performance, as well as evaluating operators and maintenance personnel.

4.2.2 Plant-specific safety decisions

The USNRC has made PRA-based analysis part of its basis for safety decisions. Since the *Reactor Safety Study*, at least four PRAs for plants at high population sites—the Zion plant in Illinois [14], the Indian Point station in New York [15], the Limerick generating station in Pennsylvania [38], and the Millstone Unit 3 in Connecticut—have been conducted at the request of the USNRC due to safety concerns. The policy statement on severe accidents issued in 1985 [11] further requires that the applicant of a new design for a nuclear power plant (or a proposed custom plant in the future) submit a complete PRA in which the severe accident vulnerabilities of the plant and their impact on public risks are considered. More recently, in the generic letter on IPE issued in 1988, the USNRC staff requested that an IPE be performed at each licensed nuclear power plant in order to provide sufficient information on the assessment of severe accident vulnerabilities [39]. The use of PRA is one of the methods approved by the USNRC to perform this examination.

Some PRAs are also initiated by utilities in response to regulatory requirements, as the utilities see that the benefits of doing PRAs outweigh their costs. Two such applications of PRAs, the Big Rock Point PRA by the Consumers Power Company [40] and the Seabrook PRA by the Public Service Company of New Hampshire and Yankee Atomic Electric Company [41], will be discussed in the next section.

4.3 The utility use of PRA

The utility use of PRA has a diverse track record [42]. Factors determining the success of a PRA program include the size and the purpose of the program, the technical methods and tools used in the analysis, and the relationship between the PRA team and the rest of the utility organization. While some utilities have experienced apparent success and have gained benefits from the performance and application of PRA, other utilities did not find that the benefits of PRA justified its cost. The situation is made even more obscure in that the application of PRA results is seldom documented, and that its benefits are rarely compared with its costs. In Von Herrmann et al. [42] made several attempts to track down some of the characteristics which enhanced or hindered the success of PRA applications. In the following, we discuss some practical benefits that utilities received from their PRA programs.

4.3.1 Demonstration of plant safety

As mentioned previously, under the requirement of the USNRC, four full scale PRAs of plants at high population sites—Zion, Indian Point, Limerick and Millstone Unit 3—were carried out to demonstrate that the risks imposed by these plants to the public are negligible small. In addition to these PRAs, some utilities chose to do PRAs on a volunteer basis prior to the application for their operating licenses of nuclear power plants or even after their plants had started operation. These utilities, in general, believe that their PRA programs would either have an important impact on whether they would receive their operating licenses, or allow them to establish a good reputation with the USNRC and the public by demonstrating the safe operation of their nuclear power plants in the analyses.

An example of a voluntary PRA is the *Seabrook Station Probabilistic Safety Assessment* (SSPSA) [41] performed for the Public Service Company of New Hampshire and the Yankee Atomic Electric Company of Massachusetts. In this report, the station was demonstrated to impose a much smaller risk to public health and safety than other man-made and natural sources of risk to which public was already exposed, and its emergency planning zone was shown to be appropriate. This supported the decision made by the USNRC to allow the issuance of a full power license to the plant. On March 1, 1990, a belated full-power operating license for the Seabrook nuclear unit in New Hampshire was granted to the Public Service Company of New Hampshire and the Yankee Atomic Electric Company of Massachusetts by the USNRC.

4.3.2 Support of safety evaluations

Probabilistic risk assessments have been demonstrated to be an effective tool in providing safety insights that are not attainable through other means of safety analysis. The Oconee PRA study [43], for an example, concluded that the dominant contributor to its core melt frequency was flooding in the turbine building. This specific event had been previously identified by Duke Power Company as an important safety concern, and actions were taken for steam generator cooling and reactor coolant makeup. The PRA study, however, not only confirmed this concern, but also provided a detailed understanding of the phenomenon and the timing of the accident sequences following this particular initiating event. It allowed the utility to make relatively inexpensive modifications that significantly reduced the core melt frequency.

The application of the Big Rock Point PRA [40] is an example opposite to that of Oconee PRA. The PRA technique was also used in this case to identify plant-specific safety concerns and define cost-beneficial modifications to accommodate these concerns. The Big Rock Point study, however, concluded that it would be either ineffective or not cost effective for the plant to follow the post-TMI action plan suggested by the USNRC to improve plant safety. Instead, the study recommended several design changes other than those recommended in the post-TMI action plan, and one procedural change that would be much more cost effective from the safety point of view.

4.3.3 Evaluation of plant modifications

Some utilities have routinely used PRA techniques to evaluate the safety impact of modifications made on plant hardware systems or to operating procedures. Northeast Utilities, for example, has developed and implemented a comprehensive PSA program in support of nuclear power plant engineering and operation. All design changes at nuclear power plants under the control of Northeast Utilities are required to include PSA reviews at both the conceptual stage and the final stage. Among the dozens of design reviews since the implementation of this requirement in early 1988, PSA analysts have recommended several proposed changes to be dropped or revised because of their negligible or reverse impact on improving public safety these were based on the findings of their PSA analyses [44].

Kazarians et al. [45] have given an example of using PRA results for fire risk analysis in risk management at a nuclear power plant. The contribution of fires to risk was found to be unacceptable in the plant under investigation, and several plant modifications were evaluated in terms of their impact on the reactor core damage frequency and public health risk. For example, Table 1 shows that the installation of fire barriers in some critical fire zones would only reduce the release frequency of radioactive material to the atmosphere by a factor of 3, while adding an alternate source of electrical power to critical components could reduce this frequency by a factor of as much as 14. These results were presented to the utility management and were part of the decision-making process. It is important to point out that the PRA results were not the only considerations in the decision; plant management had to also consider cost, operator convenience, as well as other intangible factors.

Another way of using of PRA to evaluate plant modification is to perform cost-effective analysis on alternative solutions to an identified safety issue. When a particular safety issue is identified, there is usually more than one way to address it, each associated with a given range of effects in improving plant safety and a given range of cost in implementing it. It is important from the plant management point of view that these safety issues are addressed in a most effective manner. Yankee Atomic Electric Company, for example, have used PRA techniques to identify cost-effective changes that improved the safety and reliability of the plant. The utility estimated that it had saved the stockholders several million dollars while improving overall plant safety and reliability over other approaches. Table 2 shows a sample of the benefits gained by using PRA techniques at Maine Yankee and Vermont Yankee [46].

TABLE 1

Reduction of fire risk to nuclear power plants from potential plant modifications [45]

Option	Description	Percentile	λ_{CD}[a] Events per year	Reduction factor	λ_R[b] Events per year	Reduction factor
0	Base case	5th	2.2×10^{-6}		1.5×10^{-6}	
		50th	3.0×10^{-5}		2.6×10^{-5}	
		95th	1.1×10^{-3}		9.7×10^{-4}	
		Mean	1.0×10^{-4}	1.0	9.6×10^{-5}	1.0
1	Fire barriers	5th	5.9×10^{-7}		2.1×10^{-7}	
		50th	9.1×10^{-6}		7.4×10^{-6}	
		95th	2.3×10^{-4}		2.1×10^{-4}	
		Mean	3.9×10^{-5}	2.6	3.3×10^{-5}	2.9
2	Self-contained charging pump	5th	1.6×10^{-6}		3.6×10^{-7}	
		50th	8.8×10^{-6}		3.4×10^{-6}	
		95th	9.9×10^{-5}		9.2×10^{-5}	
		Mean	1.9×10^{-5}	5.3	1.2×10^{-5}	8.0
3	Alternate power source	5th	1.7×10^{-6}		5.7×10^{-7}	
		50th	7.1×10^{-6}		3.0×10^{-6}	
		95th	4.8×10^{-5}		2.6×10^{-5}	
		Mean	1.4×10^{-5}	7.1	6.9×10^{-6}	14.0

[a] λ_{CD}: Core damage frequency, events per reactor year.

[b] λ_R: Radionuclide release frequency, events per reactor year.

4.3.4 Modification of technical specifications

The technical specifications of a nuclear power plant stipulate, for individual components and systems, the allowable outage time and surveillance requirements by which plant operation is governed and plant safety is maintained. Traditionally, the allowable outage time and the surveillance frequency of each individual component and system are determined based on engineering judgment, which is usually thought to be conservative. The current technical specifications have evolved into a complicated set of requirements, and compliance with them has been the cause of many unnecessary shutdowns. Several utilities, working through their owners groups, have attempted to use their PRAs to improve technical specifications. This includes optimization of the allowable outage time and the surveillance frequency. The Westinghouse Owners Group, for example, is currently actively involved in PRA programs that advise the utilities on ways to improve their technical specifications [47]. The utilities which employ these programs believe that these modifications, often with relaxation of technical specifications, can result in increases of plant safety,

TABLE 2

Sample of benefits gained using PRA techniques [46]

Use	Benefits	
	Safety	Economic
Electrical bus automatic loading requirements resolution (manual versus automatic control)	*Moderate*: Current design reduces probably most of automatically initiated problems	*High*: Several $100K to $1,000K saved
Reactor vessel water level system requirement resolution (Is it needed?)	*Moderate*: Proposed system reduces chances of operator error	*High*: Several $1M saved
Reactor trip breaker functional test requirements resolution (On-line testing capability versus supervisory lights)	*Moderate*: Current design is proven and has supervisory light indication	*High*: Several $100K to $1,000K saved
Safety injection system relief valve changes (Self-initiated)	*Moderate*: Eliminated two potential ECCS degradation mechanisms	*Low*: Cost $65K
Safety injection building ventilation requirements (Identified improvement potential)	*Moderate*: reduced probability that local operator actions would be required	*Low*: Cost $57K
Turbine/generator trip control changes (Added redundant trip mechanism)	*Low*: Not risk significant	*High*: Reduced frequency of d.c.-induced turbine generator failure significantly *High*: Reduced potential for rapid reactor cooling system cooldown significantly *Low*: Cost $150K
Establish risk basis for external event requirements resolution (Current requirements versus 1960 requirements)	*High*: Because it allows limited resources to be allocated more effectively	*High*: Design changes to conform to current requirements not practical

or that the increases of plant risk lie well within the tolerable safety margin. The economic savings to the utilities is, in general, expected to be substantial.

One such example is the Engineered Safety Features Actuation System Surveillance Interval and Allowable Outage Times Relaxation Program, referred to as part of the Technical Specification Optimization Program conducted in conjunction with the Westinghouse Owners Group [47]. This program was designed specifically to justify the relaxation to the surveillance intervals (SIs) and allowable outage times (AOTs) on the reactor protection system defined in the technical specification. The major motivation for such relaxation is that frequent tests often cause spurious safety injections, and stringent AOTs sometimes reduce the quality of maintenance practice. The SIs and AOTs of the base case (current requirement) and two relaxed cases (Case 1 and Case 2) for the logic cabinets, the master and slave relays, the trip breakers, and the analog channels are shown in Table 3. The changes in core damage frequency and economic saving in terms of the engineered safety features actuation system are given in Table 4. Two similar programs, the Reactor Trip Actuation System SIs and AOTs Relaxation Program and the Engineered Safety Fluid

TABLE 3

Surveillance requirements for the solid-state protection system [47]

Component	Base case	Case 1	Case 2
Logic cabinets			
Test interval (month)	2	6	2
Test time (hour)	1.5	4	4
Maintenance interval (month)	12	12	12
Maintenance time (hour)	2	12	12
Master relays			
Test interval (month)	2	6	2
Test time (hour)	1.5	4	4
Maintenance interval (month)	12	12	12
Maintenance time (hour)	2	12	12
Slave relays			
Test interval (month)	3	18	3
Test time (hour)	4	4	4
Maintenance interval (month)	12	12	12
Maintenance time (hour)	2	12	12
Trip breakers			
Test interval (month)	2	6	2
Test time (hour)	2	4	4
Maintenance interval (month)	12	12	12
Maintenance time (hour)	6	12	12
Analog channels			
Test interval (month)	1	3	3
Test time (hour)	2	4	4
Maintenance interval (month)	12	12	12
Maintenance time (hour)	1	12	12

TABLE 4

Engineered safety features actuation system results [47]

Feature	Base case	Case 1	Case 2
Core damage frequency (1/y)	4.23×10^{-5}	4.64×10^{-5}	4.33×10^{-5}
Increase in core damage frequency (%)	—	9.7	2.4
Cost savings ($/y)	—	98 600	49 900

Systems Limiting Conditions of Operation Relaxation Program (LCORP), gave similar results [47].

Within the nuclear industry, it has gradually become a common practice for many utilities to use PRA techniques in the evaluation of the proposed changes in technical specification. For example, San Onofre Nuclear Generating Station, Units 2 and 3 of Southern California Edison, has recently applied PRA techniques to evaluate a proposed change in surveillance test intervals for the auxiliary feedwater pumps from monthly to quarterly on a staggered basis [48]. The PRA evaluations have also been conducted on other plant design and procedure changes to find out their impact on plant safety. These applications have shown that PRA can provide safety-related decisions made at the nuclear power plant, based on a more rational basis.

4.3.5 Enhancement of staff capability in safe operation

Plant operation can receive benefit from PRA experience in at least two ways [42]: By increasing the safety knowledge of both engineering and operational personnel, and by using PRA results as a support for operator training. The plant engineering and operational staff, having been exposed to the integrated perspective of PRA, will have a better understanding of the design and operation of the plant as well as its safety weaknesses. The engineering and maintenance staff, on the other hand, can use PRA results to identify systems and components that are critical to plant safety, and then prioritize their quality assurance. In addition, the insights from PRA studies can be used to design control room simulator training programs that emphasize dominant accident sequences.

5. Current issues

After almost two decades of effort, PRA practitioners in the nuclear industry have achieved some success in developing a logical approach that can be systematically used for understanding and quantifying the risk associated with nuclear power plants. They have also made significant progress in convincing the nuclear regulatory agencies and many utilities that PRA techniques have great merit in providing safety insights unattainable by other means. The PRA community, however, is aware of the limitations of PRA techniques and thus focuses attention on these areas, e.g. problems related to dependent failure, human reliability, model uncertainty, expert judgment, and organizational and managerial factors. In the following, we briefly discuss the basic themes of some of these subjects and their current status of development.

5.1 Dependent failures

Both reactor operating experience and PRA results consistently indicate that dependent failures are major contributors to reactor accidents. Dependent failures, often referred to as common cause failures (CCFs), range from physical dependencies, common design and manufacturing errors to human errors. Physical dependence refers to the situation when more than one component shares the same physical location or the same supporting system, e.g. power sources or cooling systems. Events occurring at a specific physical location or a common supporting system might affect more than one component and cause multiple failures. Common design and manufacturing errors are referred to, for example, redundant components subject to loads greater than that anticipated by specification. Common human errors may occur when the same crew member performs multiple tasks, or there are flaws in operator training programs. An analysis of CCFs requires the development of models aimed to achieve one or more of three goals:
(1) qualitative evaluation of the CCF causes, from which a hierarchy of CCF causes are derived [49,50];
(2) quantitative evaluation of CCF frequencies, from which plant risk can be estimated quantitatively [51–54]; and
(3) the "cause–defense" approach [55], in which methodologies are developed to account for the impact of "plant-specific defenses", e.g. design features, and operational and maintenance policies, in order to reduce the frequency of CCFs.

The qualitative models of CCFs are useful in helping the analyst to identify the causes of existing CCFs; however, these models often face the problem of being obscure and incomplete. The real causes of many failures at the plant are hard to identify, and many others seem to have more than one potential cause. There are also failures of the same cause which occurred repeatedly with sometimes long time intervals in between. In addition, the lack of details in failure records under the current event-reporting system at most plants has made the identification of CCF causes difficult. Finally, these qualitative models are not developed to systematically identify patterns of plant maintenance, or operational policies, that have the potential to lead to CCFs prior to their actual occurrence. These shortcomings of the qualitative evaluation of CCFs have greatly limited the usefulness of such models in real application.

Most of the quantitative CCF models, on the other hand, take little interest in the causal structure of events. Instead, they are statistical models that allow free parameters to be fitted to the available data on the set of observed multiple failure events [53]. In other words, the developers of these models are more concerned with estimating correctly the frequency of CCFs and, therefore, the system unavailabilities and accident sequence frequencies, rather than the physical characteristics of CCFs. While this step is crucial to quantitative risk assessment, it provides little insight into the mechanisms of component failures of human errors, the vulnerabilities of system functions, or the ways that various factors influence the likelihood of multiple failures. Furthermore, these quantitative models, in general, fail to identify component failures or human errors that are caused by common causes rooted deeply in their cause hierarchy; and consequently, fail to correctly account the correlation between, and among, failures.

The cause–defense approach to CCFs is a new methodology, developed by the USNRC, aimed at developing methodologies to account for the impact of plant-specific defenses, e.g. design features, and operational and maintenance policies, so that the frequency of CCFs occurring at a specific plant can be reduced. It is yet to be found whether this new approach is acceptable to the nuclear industry, or is anywhere close to success in reducing the likelihood of multiple failures occurring at nuclear power plants.

5.2 Human reliability modeling

Human reliability analysis (HRA) is an integral part of PRA. It provides models for quantifying factors such as training and job environment factors, which affect human performance and thus the safety of the plant. Model development efforts in the past have centered around two parts of human behavior: human intention formation [56], which relates to how people choose their actions; and human execution of intentions, i.e. how people carry out their chosen actions.

Most of the earlier work on HRA was developed to assess the mechanisms and probabilities of execution errors, although the cognitive process was sometimes inherently included in these models. Models of this type include the USNRC handbook model [57,58], also known as "technique for human error rate prediction" (THERP); the human cognitive reliability (HCR) model [59,60]; the extended simulator data acquisition program, ultimately known as the "operator reliability experiments" (ORE) [61]; and the success likelihood index methodology–multiattribute utility decomposition (SLIM–MAUD) model [62,63]. Both the USNRC handbook model and HCR model treat human error rates as functions of the time available to the operators to act correspondingly following an event. In the absence of empirical data from operating plants, the databank of the USNRC handbook contains figures and tables that have largely been derived from subjective expert opinions. This extensive use of subjective judgment is one of the major criticisms of the USNRC handbook model [64].

The data from ORE, presumably prepared for the extensive use of the HCR model, on the other hand, relies solely on simulator data. The question raised on ORE, therefore, is whether simulator data are authentic enough to represent situations of real accidents [64]. Another critique of the HCR model, which is also applicable to ORE, is that, while addressing the stochastic uncertainties on relative response time, the model completely ignores the deviation of operator response from simulator to real events arising from the state of knowledge uncertainty, and the variation of ability from operator to operator [65]. The SLIM–MAUD model provides a highly structured approach for the derivation of human error rates using expert judgment. However, Apostolakis et al. [65] pointed out that the treatment of the weights and ratings in the SLIM–MAUD model is internally inconsistent. Beside the above-mentioned limitation, all these models on execution errors do not directly address the cognitive part of human errors, where psychologists in the HRA field have recently started their investigations aggressively.

One recently developed cognitive model in the HRA field is the cognitive reliability assessment technique (CREATE) [66], which models the human error rate in PRAs based on techniques developed in the field of artificial intelligence (AI). The model basically applies AI knowledge acquisition techniques to specify the operator's cognitive responses, and then stores them in its knowledge-base in the form of codified diagnostic rules. In this idealized AI simulator, any accident sequence can be, in principle, modeled by a set of suitable initial and boundary conditions which trigger a specific set of diagnostic rules and result in a wide spectrum of subscenarios with each subscenario having a likelihood of occurrence, P_i, which depends on the response time, t_i. CREATE provides a tool for simulating the cognitive processes that are predetermined by operator training, safety knowledge and procedural instructions, etc. However, the success of the model depends on the assumption that all brain activities and knowledge can be expressed explicitly in terms of diagnostic rules as those in the AI paradigm, and that the completeness of such a knowledge-base is attainable [64]. These drastic assumptions are remote from reality, and thus greatly limit the usefulness of the cognitive type of human reliability models.

5.3 Uncertainty in PRA

Uncertainties arise at almost every level of PRA. This is partly due to the stochastic nature of events at the plant, but, for the most part, it is due to the engineering complexity of the nuclear power system and the difficulty in modeling the physical progression of accidents. An earlier discussion of the uncertainty in PRA can be found in [67]. More recent research on uncertainty analysis not only aims at a better understanding and representation of the uncertainties at different stages of PRA, but also emphasize the development of models to reduce these uncertainties [27,68,69].

In general, the uncertainties encountered in PRAs can be grouped into two types, according to the ways that they have been introduced into the analysis: stochastic uncertainty and state-of-knowledge uncertainty [27]. The stochastic uncertainty is used to describe the random nature of the events, such as the uncertainties associated with the occurrence of initiating events and the failures of components. Since randomness is the major part of the nature of these events, increasing knowledge about the events will not be able to reduce the stochastic uncertainty. The state-of-knowledge uncertainty, on the other hand, refers to those uncertainties which arise from a lack of supporting data or a lack of clear understanding of the physical processes. The state-of-knowledge uncertainty is expected to be reduced if more data are gathered or more investigation on the specific event is carried out. For example, whether steam explosion will follow a core melt accident is currently a subject of uncertainty due to lack of sufficient knowledge of the specific event. With more experiment and analysis on the subject, steam explosion following core melt may eventually become a physical phenomenon with only stochastic uncertainty.

Most analysts agree that stochastic uncertainty can be satisfactorily modeled by the theory of probability. The model for state-of-knowledge uncertainty, however, is a more debatable subject. Traditional PRA takes the Bayesian viewpoint and represents state-of-knowledge uncertainty in terms of subjective probabilities [23,27]. Recently, some analysts have proposed that the theory of probability cannot correctly model state-of-knowledge uncertainty; instead, they turn to non-probabilistic models, such as the theory of evidence [70] and the theory of possibility [71,72]. Although it is claimed that these non-probabilistic theories have advantages over the theory of probability—for example, the ability to treat inconsistency during the process of elicitation—they cannot, nevertheless, satisfactorily answer some questions regarding modeling [73] and applications [74].

"Model uncertainty" is another area that has not attracted attention until very lately. While most of the literature deals with uncertainties that lie within the parameters of certain mathematical forms (e.g. the parameter of an exponential distribution), it is becoming increasingly evident in PRA that a major source of uncertainty could be the physical or mathematical model itself. In some cases, only several years ago, the current straightforward model was not at all obvious. For example, it is common practice now to include in the model of system unavailability the dependencies between various failures. This was not the case before the publication of *Reactor Safety Study* in 1975. System unavailabilities calculated without proper consideration of CCFs would be much smaller than the values that are typically calculated today. Even today's knowledge does not bring a consensus a a model dealing with CCFs, and different models are expected to produce different numerical values for system unavailabilities of the same system. More attention has been paid to the impact of model uncertainty on the PRA results than before, e.g. different models of CCFs and HRA are compared and discussed. Model uncertainty is still at the very early stage of its development, and there is a need for more research work on this subject in the future.

5.4 Expert opinion in PRA studies

A major problem faced by PRA analysts is the lack of statistically significant data for events of interest. Thus, PRA analysts are compelled to use expert opinions in estimating plant risks. The term "expert opinion" is used collectively in referring to any specialized knowledge, including knowledge of physical phenomena, knowledge of the design and operation of facilities, and extrapolation from the results of controlled experiments. Expert opinion has long been a subject of interest and debate [75–77]. The extensive use of expert judgment in NUREG-1150 [78,79] has, once more, attracted attention to the problems associated with the subject.

The use of expert opinion is a process typically consisting of two closely related parts: eliciting expert opinion and combining expert opinion. Since experts are often asked for opinions on subjects with uncertainty, how to best represent uncertainty almost always accompanies the issue of expert judgment. Much of the research work on eliciting expert opinion has been done by psychologists. Several notable analysts have summarized the findings from studies on the "heuristics" and "biases" behaviors, which characterize human judgment under uncertainty [80]. Because of the inevitable biases resulting from human heuristics under uncertainty when making judgments, scoring and calibration processes are important prior to the use of expert opinions. A comprehensive review from different points of view can be found in [81].

Three types of approach have been used for combining expert opinion: classical (or weighted) models [82,83], Bayesian models [84–87], and psychological scaling models [81]. All classical and psychological scaling models take ad hoc steps at one point or another. Bayesian models, on the other hand, are often too complicated and demand too much information. There is no simple and clear solution, as yet, to the problem of combining expert opinion, and the debate and interest on related issues is likely to continue.

5.5 Organizational and managerial factors

One of the major lessons learned from the Chernobyl accident is that the failure to establish a safe operational environment, through organizational and managerial policies, was one of the main contributors to the disaster [88,89]. The nature of organization and management factors affecting the safe operation of nuclear power plants can be viewed from three perspectives:

(1) they have an influence on several levels of plant operation;

(2) they include a broad range of disciplines, and through each discipline plant safety can be affected; and

(3) they affect both hardware and human reliabilities.

Up to this time, PRA methodology has not directly addressed the fact that qualities related to plant organization and management have an overall impact on plant safety. Additionally, few studies have been done on examining the correlations between plant risk and the significant characteristics of plant safety environment, such as safety knowledge of plant personnel, attitude toward plant operation, choice of plant performance goals, and lines of responsibility and communication—all of which are closely related to plant organization and management.

There are several studies aimed at developing a framework for linking management and organization elements to nuclear power plant safety [90,91], but none of these derived the quantitative relationship in between the elements. A preliminary study [92] has pointed out that the current PRA methodology can be improved in at least three ways to include organizational and managerial factors in the estimation of plant risk:

(1) By reevaluating the frequency of the "other" category of failure scenarios, of which numerical values are currently assumed to be negligible.

(2) By reassessing the probability distributions of the parameters (failure rates, human error rates, and so forth) to include organizational and managerial factors.

(3) By assessing correlations among these parameters.

Research work in this area is just beginning and is very limited.

6. Risk analysis in the chemical process industry

Unlike the extensive quantitative risk assessment (such a PRA) carried out in the nuclear power industry, the traditional approach to safety analysis in the chemical process industry has been more qualitative than quantitative. Most safety analyses for the chemical process industry in the past have focused on on-site consequences, typically in estimating plant damage and production losses. The likelihood and consequences of chemical releases were seldom analyzed or quantified. In fact, not until the major accidents at Flixborough (England), Seveso (Italy) and Bhopal (India) were the chemical process plants considered as potential major risk to the public, and not till then did the chemical process industry started thinking seriously about risk assessments at chemical plants.

A comprehensive review is given in [93,94] of recent risk evaluation procedures used in the chemical process industry. Two frequently mentioned risk evaluation methods, hazard and operability (HAZOP) analysis and quantitative risk assessment (QRA), are briefly discussed in this section. The HAZOP analysis is a systematic approach for identifying the upsets of process equipment and their effects on the functions of the process systems [93,95,96]. A HAZOP analysis team consists of experienced analysts and engineers with diverse technical backgrounds in methodology as well as plant design, construction, instrumentation, operation and maintenance. The team reviews each deviation from the normal operation at the plant and its possible causes and potential consequences. From these results the team further advises changes in design, or operation and maintenance procedures at the plant, that will improve plant safety. The HAZOP analysis is efficient in screening plant hazard. One shortcoming of this approach is that, because of its qualitative nature, its conclusions rely heavily on the subjective evaluation of the review team. Furthermore, as discussed in Section 5.1, the risk assessment of any complex system needs specifically dedicated treatment of dependent failures. Since the HAZOP analysis focuses on local equipment and operation, it is difficult to identify causes leading to multiple failures [97]. The inability to address satisfactorily the issue of dependent failure may impose a severe limitation on the usefulness of the HAZOP analysis.

Quantitative risk assessment (QRA) in the chemical process industry follows closely the approach of PRA in the nuclear industry. Figure 6 [97] shows the general approach for conducting a QRA for a chemical plant. The analysis starts with the hazard identification in which significant hazards associated with the plant, are determined. This is followed by an assessment of the frequencies and consequences of potential accident scenarios resulting from these identified hazards. Risks from various accident scenarios are then combined to determine the total plant risk, which is then used as an input for risk management decisions. More discussion on the features and models used in the three subtasks of QRA, i.e. hazard identification, frequency assessment and consequence assessment, can be found in [94,97–102].

Much of the experience learned from PRAs of nuclear power plants can be shared with risk assessments of chemical process plants. However, caution should be exercised in understanding the fundamental differences between the nature of the risks associated with nuclear plants and those associated with chemical plants. Several significant differences between the uses of PRA tech-

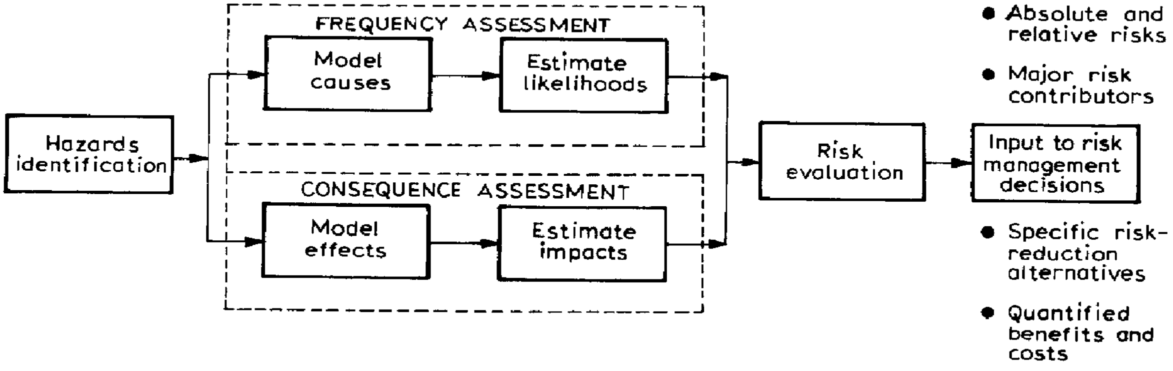
FREQUENCY ASSESSMENT
Model causes
Estimate likelihoods
Hazards identification
CONSEQUENCE ASSESSMENT
Model effects
Estimate impacts
Risk evaluation
Input to risk management decisions
• Absolute and relative risks
• Major risk contributors
• Specific risk-reduction alternatives
• Quantified benefits and costs

Fig. 6. Quantative risk assesment approach for chemical plants [97].

niques in measuring the risk in nuclear power plants and that in chemical process plants are discussed in the following paragraphs.

1. While the nuclear industry is characterized by the extensive use of redundancy and diversity for safety-related systems, the chemical industry, in general, lacks such redundancy and diversity [103]. As a result, more single failures with significant economic or environmental consequences are expected from the chemical industry than from the nuclear industry. The other consequence of lack of redundancy is the much-simplified process instrumentation in the chemical process plant [101]. This feature simplifies the development of the logic model in the system analysis of a chemical plant; on the other hand, it shifts additional responsibility for accident management onto the operating crew, which may make human error a larger contributor to the total risk in chemical plants than in nuclear plants.

2. The operation of a nuclear power plant is supervised and controlled from one central control room with an operational crew, under one superintendent, working in front of one central control panel. Chemical plants, in general, have no central supervision of the entire plant. It is common practice to have more than one control room, each controlling a specific part of the process. Furthermore, there are parts of the plant that cannot be controlled from any of the control rooms, and people have to be sent to these locations when necessary during plant operations [104]. This leads to the expectation that human reliability models for chemical process plants will be more complex than in unclear power plants.

3. The identification of hazards in chemical plants is more difficult than in nuclear plants because of the large number of hazardous locations and the variety of hazardous materials [101,103]. The nuclear power plant is characterized by a primary hazard location, i.e. the nuclear reactor core, which is also the radioactive material inventory. For plants of different design, this major concern remains the same. Experience gained in one nuclear risk assessment study provides useful information about the nature of accident sequences that are to be expected from another nuclear reactor. The chemical process industry, on the other hand, is characterized by varied inventories of hazardous chemicals located throughout its plants. Components which transport, store or process hazardous substances can be sources of different kinds of hazard, and have properties which are often unknown. The release of chemical inventories can result in a variety of hazardous reactions, many of which have consequences that are still nuclear. Consequently, while much experience can be shared among PRAs performed on nuclear power plants and attention can be focused on several hazardous locations, PRAs performed on chemical process plants have to analyze a much broader spectrum of hazardous materials. Furthermore, the fact that physical phenomena associated with each hazardous material have to be modeled individually has also made experience sharing difficult for PRAs on chemical process plants.

4. With respect to plant data, both the nuclear industry and the chemical industry have similar problems of data shortage when performing PRAs. The short history of the nuclear industry is the major reason that a sophisticated database has not yet been established. While the chemical industry has an extensive operating experience, it does not, in general, keep good records of reliable data.

5. Institutionally and culturally, the chemical industry faces more difficulties in making progress toward comprehensive and quantitative risk analysis. This industry is highly competitive and bottom-line oriented, and products and processes are often proprietary. There is also a tendency to over-simplify the analysis so that the cost of such analyses will be reduced. The results are often kept proprietary. This creates another major obstacle for PRA to become a mature and well accepted practice for risk quantification in the chemical industry [103].

7. Concluding remarks

Risk management is important for both the nuclear and the chemical industries. Before reaching any intelligent guidelines for risk management, the risks involved in each industrial sector need to be understood in terms of the three basic questions [24,102]:
(1) What can go wrong?
(2) How likely is it? and
(3) What are the consequences?
Over the last two decades, the nuclear power industry has developed an effective means for answering these questions in a comprehensive and quantitative manner through the PRA process. The successful use of PRAs has been demonstrated by increased engineering insights, improved plant safety and cost-effective recommendations. Recently, the nuclear industry has further extended the application of PRA techniques from events initiated during power operation or hot standby to events at cold shutdown or during refueling outages [105–106]. These studies provide a more complete, explicit assessment of risk at nuclear power plants to aid the making of safety-related decisions.

The chemical industry, on the other hand, has just started to look at the quantification of risk seriously within the last few years. The institutional differences between the two industries (high levels of government regulation in the nuclear industry versus competitiveness and proprietary attitudes in the chemical industry) will surely lead to a different evolution of risk assessment and management in the chemical industry.

Peer review, for example, has been found to be essential in nuclear plant PRAs. This is due to the fact that subjective judgment abounds in these studies, as discussed in this paper. The latest example of the importance of peer review is a report [107] issued by an international panel of experts which contains severe criticisms of the latest PRA from the USNRC [13]. As a result of this criticism, this PRA has been revised significantly. It would be very difficult to have such an open peer review process in the current environment under which the chemical industry operates. Given the highly subjective nature of many PRA models and, thus, the need for peer reviews, it remains to be seen how the chemical industry will handle this matter.

References

1 Reactor Safety Study, WASH-1400, NUREG-75/014, U.S. Nuclear Regulatory Commission, Washington, DC, 1975.

2 Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants, WASH-740, U.S. Atomic Energy Commission, Washington, DC, 1957.

3 F.R. Farmer, Reactor safety and siting: A proposed risk criterion, Nucl. Saf., 8 (1967) 539–548.

4 Risk Assessment Review Group, Report to the U.S. Nuclear Regulatory Commission, NUREG/CR-0400, U.S. Nuclear Regulatory Commission, Washington, DC, 1978.

5 USNRC Statement on Risk Assessment and the Reactor Safety Study Report, WASH-1400, in Light of the Risk Assessment Review Group Report, U.S. Nuclear Regulatory Commission, Washington, DC, January 18, 1979.

6 J.G. Kemeny, Report of the President's Commission on the Accident at Three Mile Island, Washington, DC, 1979.

7 M. Rogovin, Three Mile Island—A Report to the Commissioners and to the Public, NUREG/CR-1250, U.S. Nuclear Regulatory Commission, Washington, DC, 1980.

8 PRA Procedures Guide—A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, NUREG/CR-2300, Vols. 1 and 2, American Nuclear Society and U.S. Nuclear Regulatory Commission, Washington, DC, 1983.

9 Probabilistic Risk Assessment Reference Document, NUREG-1050, U.S. Nuclear Regulatory Commission, Washington, DC, 1984.

10 M. Silberberg, Reassessment of the Technical Bases for Estimating Source Terms, NUREG-0956, U.S. Nuclear Regulatory Commission, Washington, DC, 1986.

11 U.S. Nuclear Regulatory Commission, Policy statement on severe reactor accident regarding future design and existing plants, Federal Register, 50 (1985) 32 138.

12 U.S. Nuclear Regulatory Commission, Safety goals for the operation of nuclear power plants. policy statement, Federal Register, 51 (1986) 30 028.

13 Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants (Second Draft for Peer Review), NUREG-1150, Vols. 1 and 2, U.S. Nuclear Regulatory Commission, Washington, DC, 1989.

14 Commonwealth Edison Company, Zion Probabilistic Safety Study (Unit 1), Vols. 1–10, Docket 50-295, No. 8109 280 415 (-8109 280 420), 1981, available at NRC Public Document Room, Washington, DC.

15 Consolidated Edison Company and New York State Power Authority, Indian Point Probabilistic Safety Study, Vols. 1–12, Dockets 50-247 (Unit 2) and 50-286 (Unit 3), No. 8203 110 003 (-8203 110 004), 1982, available at NRC Public Document Room, Washington, DC.

16 GRS, Deutsche Risikostudie Kernkraftwerke, Hauptband und Fachbände, Verlag TÜV Rheinland, 1979 (English translation: German Risk Study, Main Report, EPRI NP-1804-SR, Electric Power Research Institute, Palo Alto, CA, 1981).

17 P.J. Ross, An overview of the PSA for the Sizewell 'B' power station, In: Proc. International Topical Meeting on Probability, Reliability and Safety Assessment, PSA '89, Pittsburgh, PA, April 2-7, 1989, American Nuclear Society, La Grange Park, IL, 1989, pp. 769-776.

18 S. Kaplan, Matrix theory formalism for event tree analysis: application to nuclear risk analysis, Risk Anal., 2 (1982) 9-18.

19 D.P. Mackowiak, C.D. Gentillon and K.L. Smith, Development of Transient Initiating Event Frequencies for Use in Probabilistic Risk Assessment, NUREG/CR-3862 (EGG-2323), U.S. Nuclear Regulatory Commission, Washington, DC, 1985.

20 A.J. Oswald, Generic Data Base for Data and Models Chapter of the National Reliability Evaluation Program (NREP), EGG-EA-5887 (Interim Report), EG&G Idaho, Inc., Idaho Falls, ID, 1982.

21 W.E. Vesely, F.F. Goldberg, N.H. Roberts and D.F. Haasl, Fault Tree Handbook, NUREG-0492, U.S. Nuclear Regulatory Commission, Washington, DC, 1981.

22 J.B. Fussell, Fault tree analysis—Concepts and techniques, In: E.J. Henley and J.W. Lynn (Eds.), Generic Techniques in Systems Reliability Assessment, Wolters-Noordhoff, Leiden, 1976, pp. 133-162.

23 G. Apostolakis, Probability and risk assessment: The subjectivistic viewpoint and some suggestions, Nucl. Saf., 19 (1978) 305-315.

24 S. Kaplan and B.J. Garrick, On the quantitative definition of risk, Risk Anal., 1 (1981) 11-27.

25 B. de Finetti, Theory of Probability, Vols. 1 and 2, John Wiley and Sons, New York, NY, 1974.

26 D. Dubois and H. Prade, Recent models of uncertainty and imprecision as a basis for decision theory: Towards less normative frameworks, In: E. Hollnagel, G. Mancini and P.D. Woods (Eds.), Intelligent Decision Support in Process Environments, Springer-Verlag, Berlin, 1985, pp. 1-24.

27 G. Apostolakis, Uncertainty in probabilistic safety assessment, Nucl. Eng. Des., 115 (1989) 173-179.

28 G. Apostolakis, Data analysis in risk assessment, Nucl. Eng. Des., 71 (1982) 375-381.

29 G. Apostolakis, Bayesian methods in risk assessment, In: J. Lewins and M. Becker (Eds.), Advances in Nuclear Science and Technology, Vol. 13, Plenum, New York, NY, 1981, pp. 415-465.

30 Domestic Licensing of Production and Utilization Facilities, 10CFR50, U.S. Nuclear Regulatory Commission, Washington, DC, 1978.

31 V. Joksimovich, A review of plant specific PRAs, Risk Anal., 4 (1984) 255-266.

32 V. Joksimovich, An overview of insights gained and lessons learned for U.S. plant-specific PRA studies, Nucl. Saf., 27 (1986) 15-27.

33 B.J. Garrick, Lessons learned from 21 nuclear plant PRA, In: Proc. Int. Topical Meeting on Probabilistic Safety Assessment and Risk Management, PSA '87, Zurich, Switzerland, August 30-September 4, 1987, Verlag TÜV Rheinland GmbH, Köln, 1987, pp. 369-383.

34 W.W. Weaver, Deterministic criteria versus probabilistic analyses: Examining the single failure and separation criteria, Nucl. Technol., 47 (1980) 234-243.

35 W.W. Weaver, Pitfalls in current design requirements, Nucl. Saf., 22 (1981) 328-336.

36 M.L. Ernst and J.A. Murphy, Risk assessment of regulation of nuclear power plants, Mech. Eng., November (1984) 31-35.

37 R. Emrit, Prioritization of Generic Safety Issues, NUREG-0933, U.S. Nuclear Regulatory Commission, Washington, DC, 1983.

38 Philadelphia Electric Company, Severe Accident Risk Assessment: Limerick Generating Station, Vols. 1-4, Dockets 5-352 (Unit 1) and 50353 (Unit 2), No. 8304 220 103 (-8304 220 108), 1983, available at Nuclear Regulatory Commission Public Document Room, Washington, DC.

39 Individual Plant Examination for Severe Accident Vulnerabilities, Generic Letter No. 88-20, U.S. Nuclear Regulatory Commission, Washington, DC, November 23, 1988.

40 Consumers Power Company, CPC Probabilistic Risk Assessment: Big Rock Point, USNRC Docket 50-155, Washington, DC, 1981.

41 Pickard, Lowe and Garrick, Inc., Seabrook Station Probabilistic Safety Assessment, prepared for Public Service Company of New Hampshire and Yankee Atomic Electric Company, PLG-0300, Newport, CA, 1983.

42 J.L. von Herrmann, P.J. Wood, J.P. Gaertner and I.B. Wall, The practical application of PRA: An evaluation of utility experience and USNRC perspectives, Reliability Eng. Syst. Saf., 24 (1989) 167–198.

43 Electric Power Research Institute, Nuclear Safety Analysis Center and Duke Power Company, A Probabilistic Risk Assessment of Oconee Unit 3, Report NSAC-60, Palo Alto, CA, 1984.

44 D.A. Dube, PSA support of nuclear power plant engineering and operations, In: Proc. International Topical Meeting on Probability, Reliability and Safety Assessment, PSA '89, Pittsburgh, PA, April 2–7, 1989, American Nuclear Society, La Grange Park, IL, 1989, pp. 443–452.

45 M. Kazarians, N.O. Siu and g. Apostolakis, Risk management application of fire risk analysis, In: C.E. Grant and P.J. Pagni (Eds.), Proc. of First Int. Symp. on Fire Safety and Science, National Bureau of Standards, Gaithersburg, MD, October 7–11, 1985, Hemisphere, New York, NY, 1985, pp. 1029–1038.

46 J.R. Chapman, Yankee Atomic Electric Company uses of PRA, In: Proc. Int. Topical Meeting on Probability, Reliability and Safety Assessment, PSA '89, Pittsburgh, PA, April 2–7, 1989, American Nuclear Society, La Grange Park, IL, 1989, pp. 453–459.

47 G.R. Andre, M.J. Hitchler, N.J. Liparuto and R.K. Rodibaugh, The use of probabilistic risk assessment to obtain LCO and surveillance frequency relaxation, In: Proc. Int. Topical Meeting on Probability, Reliability and Safety Assessment, PSA '89, Pittsburgh, PA, April 2–7, 1989, American Nuclear Society, La Grange Park, IL, 1989, pp. 427–432.

48 Southern California Edison, PRA Evaluation of Extension of the Monthly Surveillance Test Interval for the SONGS 2/3 Auxiliary Feedwater Pumps, NSG/PRA Report PRA-2/3-90-023, 1990.

49 I.A. Watson and G.T. Edwards, Common-mode failures in redundancy systems, Nucl. Technol., 46 (1979) 180–185.

50 Los Alamos Technical Associates, Inc., Common Cause Failures—Phase I: A Classification System, EPRI NP-3383, Electric Power Research Institute, Palo Alto, CA, 1984.

51 K.N. Fleming, A. Mosleh and R.K. Deremer, A systematic procedure for the incorporation of common cause events into risk and reliability models, Nucl.Eng. Des., 93 (1986) 245–273.

52 G. Apostolakis and P. Moieni, The foundations of models of dependence in probabilistic safety assessment, Reliability Eng., 18 (1987) 177–195.

53 G.W. Parry, On models of causal dependency, In: Proc. 10th Int. Conf. on Structural Mechanics in Reactor Technology, Anaheim, CA, August 14–18, 1989, Vol. P, pp. 57–62.

54 A. Mosleh, K.N. Flemming, G.W. Parry, H.M. Paula, D.H. Worledge and D.M. Rasmuson, Procedures for Treating Common Cause Failures in Safety and Reliability Studies, NUREG/CR-4780 (EPRI NP-5613), U.S. Nuclear Regulatory Commission, Washington, DC, 1988.

55 H.M. Paula and G.W. Parry, A Cause–Defense Approach to the Understanding and Analysis of Common Cause Failures, NUREG/CR-5460, U.S. Nuclear Regulatory Commission, Washington, DC, 1990.

56 D.D. Wood, E.M. Roth and H. People, Jr., Modeling human intention formation for human reliability assessment, Reliability Eng. Syst. Saf., 22 (1988) 169–200.

57 A.D. Swain and H.E. Guttmann, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Applications, NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington, DC, 1983.

58 A.D. Swain, Accident Sequence Evaluation Program Human Reliability Analysis Procedure, NUREG/CR-4772, U.S. Nuclear Regulatory Commission, Washington, DC, 1987.

59 G.W. Hannaman, V. Joksimovich, D.H. Worledge and A.J. Spurgin, The role of human reliability analysis for enhancing crew performance, in Proc. International ANS/ENS Topical Meeting on Advances in Human Factors on Nuclear Power Systems, Knoxville, TN, 1986, American Nuclear Society, La Grange Park, IL, 1986.

60 G.W. Hannaman and A.J. Spurgin, Systematic Human Action Reliability Procedure (SHARP), EPRI NP-3583, Electric Power Research Institute, Palo Alto, CA, 1984.

61 V. Joksimovich, A.J. Spurgin, D.D. Orvis and P. Moieni, EPRI operator reliability experiments program: model development/testing, In: Proc. Int. Topical Meeting on Probability, Reliability and Safety Assessment, PSA '89, Pittsburgh, PA, April 2–7, 1989, American Nuclear Society, 1989, pp. 120–127.

62 D.E. Embrey, P.C. Humphreys, E.A. Rosa, B. Kirwan and K. Rea, SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment, NUREG/CR-3518, U.S. Nuclear Regulatory Commission, Washington, DC, 1984.

63 D.E. Embrey, SLIM-MAUD: A computer-based technique for human reliability assessment, In: Proc. Int. ANS/ENS Topical Meeting on Probabilistic Safety Methods and Applications, San Francisco, CA, American Nuclear Society, 1985.

64 E.M. Dougherty, Jr., Human reliability analysis—Where shouldst thou turn? Reliability Eng. Syst. Saf., 29 (1989) 283–299.

65 G.E. Apostolakis, V.M. Bier and A. Mosleh, A critique of recent models for human error rate assessment, Reliability Eng. Syst. Saf., 22 (1988) 201–217.

66 D.D. Woods, E.M. Roth and H. Pople, Jr., Models of Cognitive Behavior in Nuclear Power Plant Personnel, NUREG/CR-4532, U.S. Nuclear Regulatory Commission, Washington, DC, 1986.

67 G.W. Parry and P.W. Winter, Characterization and evaluation of uncertainty in probabilistic risk analysis, Nucl. Saf., 22 (1981) 28–42.

68 G.W. Parry, Technical Note: On One Type of Modeling Uncertainty in Probabilistic Risk Assessment, Nucl. Saf., 24 (1983) 624–627.

69 G.W. Parry, Use of judgment in representing uncertainty in PRAs, Nucl. Eng. Des., 93 (1986) 135–144.

70 G. Shafer, A Mathematical Theory of Evidence, Princeton University Press, Princeton, NJ, 1976.

71 D. Dubois and H. Prade, Possibility Theory: An Approach to Computerized Processing of Uncertainty, Plenum Press, New York, NY, 1988.

72 L.A. Zadeh, Fuzzy sets, Inform. Control, 8 (1965) 338–353.

73 J.F.J. van Steen and P.D. Oortman Gerlings, Expert Opinions in Safety Studies, Vol. 2: Literature Survey Report, Delft University of Technology, Delft, Netherlands, 1989.

74 J.S. Wu, G.E. Apostolakis and D. Okrent, Uncertainties in system analysis: Probabilistic versus nonprobabilistic theories, Reliability Eng. Syst. Saf., 30 (1990) 163–181.

75 G. Apostolakis (Ed. Special Issue), The interpretation of probability in probabilistic safety assessments, Reliability Eng. Syst. Saf., 23 (1988) 247–320.

76 A. Mosleh, V.M. Bier and G. Apostolakis, A critique of current practice for the use of expert opinions in probabilistic risk assessment, Reliability Eng. Syst. Saf., 20 (1988) 63–85.

77 G. Apostolakis, Expert judgment in probabilistic safety assessment, In: D.V. Lindley and C.A. Clarotti (Eds.), Accelerated Life Testing and Expert Opinions in Reliability, Elsevier, Amsterdam, 1988, pp. 116–131.

78 T. Wheeler, S.C. Hora and W.R.C. Cramond, Analysis of Core Damage Frequency from Internal Events: Expert Judgment Elicitation, NUREG/CR-4550, Vol. 2, U.S. Nuclear Regulatory Commission, Washington, DC, 1988.

79 Ortiz, et al., Use of expert judgment in NUREG-1150: In: Proc. Int. Topical Meeting on Probability, Reliability and Safety Assessment, PSA '89, Pittsburgh, Pennsylvania, April 2–7, 1989, American Nuclear Society, La Grange Park, IL, 1989, pp. 581–592.

80 A. Tversky and D. Kahneman, Judgment under uncertainty: Heuristics and biases, In: D. Kahneman, Slovic and A. Tversky (Eds.), Judgment Under Uncertainty, Cambridge University Press, Cambridge, U.K., 1982.

81 R.M. Cooke, Experts in Uncertainty: Expert Opinion and Subjective Probability in Science, Delft University of Technology, Delft, Netherlands, 1989.

82 R. Winkler, The consensus of subjective probability distributions, Manag. Sci., 15 (1968) 861–875.

83 R. Winkler, Scoring rules and the evaluation of probability assessors, J. Am. Stat. Assoc., 64 (1969) 1073–1078.

84 A. Mosleh and G. Apostolakis, The assessment of probability distributions from expert opinions with an application to seismic fragility curves, Risk Anal., 6 (1986) 447–461.

85 P. Morris, Combining expert judgments: A Bayesian approach, Manag. Sci., 23 (1977) 679–693.

86 P. Morris, An axiomatic approach to expert resolution, Manag. Sci., 29 (1983) 24–32.

87 S. French, Group consensus probability distribution: A critical survey, Bayesian Statist., 2 (1985) 183–202.

88 Report on the Accident at the Chernobyl Nuclear Power Station, NUREG-1250, U.S. Nuclear Regulatory Commission, Washington, DC, 1987.

89 J. Reason, Errors and Violations: The Lessons of Chernobyl, presented at the IEEE 4th Conf. on Human Factors and Power Plants, Monterey, CA, June 5–9, 1988.

90 A.A. Marcus, Management, Organization and Safety in Nuclear Power Plants, U.S. Nuclear Regulatory Commission, Washington, DC, 1990.

91 R. Osborn, Organizational Analysis and Safety for Utilities with Nuclear Power Plants, NUREG/CR-3215, U.S. Nuclear Regulatory Commission, Washington, DC, 1983.

92 J.S. Wu, G.E. Apostolakis and D. Okrent, On the Inclusion of Organizational and Managerial Influences in Probabilistic Safety Assessments of Nuclear Power Plants, presented at the Society for Risk Analysis Annual Meeting, San Francisco, CA, October 29–November 1, 1989.

93 Guidelines for Hazard Evaluation Procedures, American Institute of Chemical Engineers, Center for Chemical Process Safety, New York, NY, 1985.

94 Guidelines for Chemical Process Quantitative Risk Analysis, American Institute of Chemical Engineers, Center for Chemical Process Safety, New York, NY, 1989.

95 R.E. Knowlton, An Introduction to Hazard and Operability Studies, Chemetics International Company, Vancouver, B.C., 1987.

96 A Guide to Hazard and Operability Studies, Chemical Industries Assoc., London, 1977.

97 D.F. Montague, Process risk evaluation—What method to use? Reliability Eng. Syst. Saf., 29 (1990) 27–53.

98 G.R. Van Sciver, Quantitative risk analysis in the chemical process industry, Reliability Eng. Syst. Saf., 29 (1990) 55–68.

99 M.T. Mills and R.J. Paine, A survey of modeling techniques for consequence analysis of accidental chemical releases to the atmosphere, Reliability Eng. Syst. Saf., 29 (1990) 69–102.

100 S.R. Hanna and P.J. Drivas, Guidelines for Use of Vapor Cloud Dispersion Models, American Institute of Chemical Engineers, Center for Chemical Process Safety, New York, NY, 1987.

101 P. Guymer, G.D. Kaiser and T.C. Mckelvey, Probabilistic risk assessment in the CPI, Chem. Eng. Prog., January (1987) 37–45.

102 J.S. Arendt, Using quantitative risk assessment in the chemical process industry, Reliability Eng. Syst. Saf., 29 (1990) 133–149.

103 B.J. Garrick, The approach to risk analysis in three industries: nuclear power, space systems and chemical process, Reliability Eng. Syst. Saf., 23 (1988) 195–205.

104 K.E. Petersen, Risk Analysis Uses and Techniques in the Non-nuclear Field: A Nordic Perspective, Nordic Liaison Committee for Atomic Energy, Denmark, February, 1986.

105 J.H. Moody, Jr., T.J. Casey and K.L. Kiper, Seabrook Station Probabilistic Safety Study Shutdown Modes 4, 5 and 6, In: Proc. Int. Topical Meeting on Probability, La Grange Park, IL, Reliability and Safety Assessment, PSA '89, Pittsburgh, PA, April 2–7, 1989, American Nuclear Society, 1989, pp. 438–442.

106 Southern California Edison, Safety Assessment of the San Onofre Nuclear Generating Station, Unit, Cycle 11 Refueling Outage, July 1990.

107 W.E. Kastenberg, G. Apostolakis, et al., Findings of the Peer Review Panel on the Draft Reactor Risk Reference Document (NUREG-1150), USNRC Report NUREG/CR-5113, U.S. Nuclear Regulatory Commission, Washington, DC, 1988.