IChem^E

0957–5820/99/$10.00+0.00
© Institution of Chemical Engineers
Trans IChemE, Vol 77, Part B, May 1999

THE EVOLUTION OF PROBABILISTIC RISK ASSESSMENT IN THE NUCLEAR INDUSTRY

M. R. HAYNS

School of Engineering and Applied Science, Aston University, Birmingham, UK

The use of probabilistic methods for evaluating the performance of plant is now commonplace. In the nuclear industries it has undergone a vigorous period of development and is now considered by its aficionados to be a mature topic. It may be considered technically mature in that methods and data have been refined considerably and its positive and negative points are well understood. However, its breadth of application, especially in its most complex forms when risk rather than reliability is evaluated, has not been as wide as originally hoped, especially as an aid to regulation as in the evaluation of risk acceptance, or tolerability.

This paper follows the development of that set of analytical techniques which together form probabilistic risk (or safety) assessment through its most formative years (1975–1985) by means of examples drawn from the definitive calculations of the period– in particular, the Reactor Safety Study (1975), the Zion and Indian Point studies in the USA and the Sizewell B study in the UK (all circa 1983). All of these studies contributed in specific ways to the development of the methods. In addition, the Sizewell B study, through its use in a public enquiry, also precipitated a debate on the use and interpretation of the results in the public domain.

This evolution clearly shows both the power of the methods, and their extreme complication. These aspects have contributed to the current status of the methods, both for plant performance and regulatory interpretations, and to the prospects for further developments.

Keywords: nuclear power; probabilistic methods; risk assessment; tolerability of risk; severe nuclear accident methodology.

1. INTRODUCTION

The use of probabilistic methods for evaluating plant performance is now very common. In the nuclear industries it has undergone a vigorous period of development and in many ways is considered as a ‘mature topic’. In fact, as the history of its development shows, it has served primarily to highlight some key features of plant *reliability*, shown the enormous complexity and challenge in being able to fully characterize components and system performance in conditions well beyond their designed-for capabilities, and exposed the deep philosophical problems associated with defining acceptability (or tolerability) of risks, both technically and in the public domain. This review attempts to show how the methods have been developed, primarily with reference to the needs of the nuclear industry. The other reviews accompanying it in this issue address the origins and history of loss prevention, and developments in the offshore oil and gas industry. There are many points of overlapping interest, and some of the synergies will be brought out. The vexed question of comparative risk assessment, either between nuclear and other industrial risks or between human actions and natural events, is left to further discussion.

I have used the term ‘Probabilistic Risk Assessment’ (PRA) in the title. This is synonymous with the more modern usage of Probabilistic *Safety* Assessment (PSA) and is also the same as Quantitative Risk Assessment (QRA), which is the terminology favoured by non-nuclear applications. They are all similar in that they require quantification of both the frequency (or probability) of an undesired event, and its consequences. For consistency I have used ‘PSA’ throughout this review.

The International Atomic Energy Agency (IAEA) has rather formally defined PSA as ‘The appropriate application of Probabilistic Risk Assessment (PRA) to safety decisions’[1]. As will be seen, it is not necessarily the quantification of *risk* which the most useful parameter, and indeed it has been the difficulties in characterizing risk, and particularly the associated uncertainties, which have held back the more general use of the methodology.

Whilst the concept of ‘risk’ is understood in a visceral sense by most people, it is in fact a very tenuous thing when attempts are made to give it a rigorous definition. Thus, the ‘dictionary’ definition is simply ‘a hazard, or the chance of commercial loss’[2]. This is not very illuminating. There have been a number of attempts by well-qualified technical professionals to provide a more rigorous definition. Thus, in 1983, The Royal Society Study Group offered a much-quoted definition[3]:

‘For the purposes of this report the Study Group views RISK as the probability that a particular adverse event occurs during a stated period of time, or results from a particular challenge.

An ADVERSE EVENT is an occurrence that produces harm. With RISK defined as above, HAZARD is seen as the situation that in particular circumstances could lead to harm, where HARM is the loss to a human being or to a human population consequent on the damage and DAMAGE is the loss of inherent quality suffered by an entity (physical or biological).
BENEFIT is the gain to a human population.
DETRIMENT is a numerical measure of the expected harm or loss associated with an adverse event.'

This definition or group of definitions is rather general, though comprehensive. A set of definitions more suitable for use in the chemical process industries has been developed by the Institution of Chemical Engineers (IChemE)[4].

'HAZARD: a physical situation with a potential for human injury, damage to property, damage to the environment or some combination of these.
RISK: the likelihood of a specified undesired event occurring within a specified period or in specified circumstances. It may be either a *frequency* (the number of specified events occurring in unit time) or a *probability* (the probability of a specified event following a prior event), depending on the circumstances.'

These two definitions (or sets of definitions) are typical of a number that have been produced, but are essentially of the same type. The difference between them shows the desirability of using the terms which are most suitable in a particular context. For example, in its book *Living with Risk*[5] the British Medical Association chose the Royal Society Study Group Definition.

For use in the application to the nuclear industry it has been suggested[6] that an adaptation of the IChemE definition is the most useful– that is:

'RISK; the likelihood of specified undesired events occurring within a specified period or in specified circumstances arising from the realisation of a specified hazard. It may be expressed as either a frequency (the expected number of specified events occurring in unit time) or a probability (the probability of a specified event following a prior event), depending on the circumstances.'

This definition indicates that the analysis is concerned with a range of possible accident-initiating events which could cause different types of harm and to differing extents.

Although all the quotations above mention probabilities in their definitions, they do not define what is meant. In fact the nature of probability– which defines the nature of risk– has been a topic of debate by mathematicians and philosophers ever since its concepts were first applied. I do not wish to get into this in any detail; the definitions are simply saying that risk is represented quantitatively using the algebra of probability[7].

The three types of probability which occur when estimating the risk posed by nuclear plant are:

- those obtained directly from observations (such as the statistics of component failures);
- those obtained by logical deduction (with such techniques as the fault or event trees of probabilistic safety assessment);
- those expressing degrees of belief (such as arise from the techniques used to extract expert opinion).

The nature of these three types of probability, as well as the difference between frequency and probability, need to be borne in mind whenever discussion of risk, and particularly its quantification, are undertaken.

A very useful compendium of definitions and generic terms and concepts relating to risk is available[8].

The Evolution of the Concept of Risk

The concept of risk has, of course, a very long history and has been extensively reviewed (see for example References 9 and 10). The picture is generally of the concept of risk evolving from exposure to misfortune on the vagaries of our natural environment to exposure to industrial hazards and other man-made activities. Thus, the concept of risk is deeply embedded in our cultural heritage. That much of the early evaluation of risk as a concept was closely linked with the development of religious thought, especially the probability of the after-life, should give the modern student of the subject a strong forewarning that these are deep and difficult waters.

The concepts of insurance and home commercial risk management have a history almost as long as the concept of risk itself, but the real milestone came with the development of probability theory by Pascal in 1657. This seems to have initiated a flurry of activity culminating in the first quantitative assessment of risks to health which would be recognized by modern practitioners– LaPlace's analysis of the influence of smallpox vaccinations on the probability of death in 1792.

An appreciation of the risk to the environment as a variant of the concept of risk to people began to emerge only later. (I leave aside many early assessments of risk to farmers from flooding, pestilence and so on.) Indeed, the connection between risks to man and risks to the environment, and hence the concept of the symbiosis between man and his environment, came later still. This is described in Lord Ashby's seminal book on environmental risk[11]. The attainment of a society with time and wealth to appreciate the natural environment seems to have been a prerequisite for such a development. Perhaps the most eloquent example of such thinking is to be found in Rousseau's *Nightingale*, as cited by Ashby. Rousseau asks to what lengths we should go to have the pleasure of hearing the nightingale.

As we come closer to the present time, and particularly the last decades, the amount of literature expands enormously and the historical perspective is lost. However, the concept of 'risk' does seem to have continued to evolve, and certainly the common usage of the word is in flux. The emergence of the environmental movement has served to focus on the relationship between man and his environment to the point where it is no longer simply the impact of an activity on people that is of concern, but rather the wider feeling that we must be cognisant of the need to protect our total environment that is of prime importance. These are not altruistic or sentimental feelings. The clear interdependence of all life on earth is now widely accepted, though few would go quite as far as Lovelock with the concept of Gaia. This movement has Rachel Carson's *Silent Spring* as one of its influential milestones. Whether or not we agree with the technical details of works such as this, we must accept that they have significantly affected the intellectual climate in which we now work, and we should attempt to express goals in terms which properly match the public's perception of these matters.

This brings the development of the concept of risk to the present. We have finally introduced the idea of *perception* of risk. Risk cannot be felt (although fear can) and it is essentially unmeasurable. It can, however, be calculated, albeit imperfectly, and this leads to further problems. Take, for example, the question of life expectancy. This has improved enormously this century. Increases of about 20 years have been achieved in Western Europe and North America[5]. Despite this, reductions in the frequency of catastrophic events and continuing assurances that the health of the population is getting better, people constantly indicate through polls and other sampling techniques that they believe life is getting riskier.

Furthermore, continuing scientific investigations are bringing new and previously unknown risks to the attention of the public, creating an impression of an environment becoming increasingly hazardous for its inhabitants. Research into the factors controlling people's perception of risk has indicated that the primary attributes for public concern are not mortality or morbidity rates, which seem remote, but characteriztics such as the potential for catastrophe; lack of familiarity and understanding; the involuntary nature of risks; scientific uncertainty; lack of personal control; risks to future generations; doubtful benefits; inequitable distribution of risks and benefits; and potentially irreversible effects. When coupled with the dread of nuclear matters associated with weapons and the 'mystery' of radiation in general, these factors give some insights as to why the generation of electricity by nuclear fission is bearing the brunt of the debate concerning risks to society from the activities of advanced technological industries.

The evolution of 'risk' as a component of our culture has been presented above from the rather parochial view of Western cultural development. Any consideration of the acceptability (or tolerability) of risk is therefore dependent on the cultural values existing in a society. Of particular concern is the relationship between purely economic factors (essentially a matter of insurance) and other aspects of society. Thus, the value attributed to human life has important ramifications when judgements are made as to the costs which would be considered appropriate to improve the safety of plant, and hence save lives. Different nations and cultures might have differing approaches to the issues of the cost of life and the balance between the desire to develop technologies with the potential for great benefit and the need to make plant safe. I shall not go into this, but note that I am addressing this issue from the perhaps parochial needs of an industry operating in the conditions of the Western or developed nations.

This evolution of our 'cultural' understanding of risk is important because any calculations aimed at quantifying the risk posed by particular activities must be 'interpretable' in terms of current usage. As will be seen, one of the outcomes of using PSA results in the public domain has been to fuel the debate over the acceptability of nuclear activities rather than, as the purely technical interpretation of the results would seem to suggest, give members of the public confidence that they are not seriously threatened by them.

The Beginnings of Quantification of Risk and Reliability

An understanding of the evolution of reliability engineering is as essential as PSA because it forms an important subset of the whole problem. The early days of using statistical methods for, for example, moving from single to multiple engined aircraft in the 1930s, has been documented in Green and Bourne's seminal book on reliability methods[12]. Reliability and 'Life Testing' are now well-advanced topics in their own right and are extensively used in aerospace, military and many industrial applications. For a recent overview see Kecicioglu[13]. It is *not*, however, quantitative risk assessment because it lacks any evaluation of the consequences of the failures (or, more precisely, failure rates) which it predicts. It is shown later that much of what now falls under the heading of PSA is, in fact, reliability engineering since it is the intermediate results of PSA which have become the most used– that is, those of component and systems reliability, or for the evaluation of the frequency of parameters which act as 'markers' for the performance of the system, such as core melt frequency[14].

Both the aircraft and nuclear industry were 'feeling towards a qualification of risk'[15] by the 1960s. Particular contributions were made by Siddall[16] on the reliability of various reactor components and by Howard *et al.*[17] on aircraft automatic landing.

In the UK, the Windscale accident in 1957 had an important influence on the development of the approach to safety[18]. It was not the instigator of the approach, because as early as 1955 Marley and Fry[19] made some evaluations of the consequences of possible reactor accidents so as to make sure that recommendations concerning siting and permissible levels of population in the viscinity of nuclear plant were available to decision-makers. At the same time, the designers of the first generation of nuclear power stations believed that a measure of absolute safety could be achieved by a combination of siting (limiting the number of people affected) and by reactor design (making an event leading to a release of radioactivity highly improbable). It became clear from the Windscale experience that absolute safety as envisaged could not be achieved and that there was evolving a crucial need to be able to *quantify* the risks.

It is widely accepted that Farmer made the first step towards *risk* analysis by producing, towards the end of the 1960s[20], his criteria for the permissible probabilities of releasing quantities of ^{131}I, a very volatile fission product which tends to be the most easily released following a nuclear accident. The levels are reproduced in Figure 1. The basic objective of these criteria was to ensure that less than one death to the public should be predicted for the foreseeable future arising from the operation of the then planned gas cooled reactors in the UK. By modern standards these criteria might seem very crude. Only one volatile fission product was considered, and there was no spectrum of accident sequences leading to a range of well-characterized releases. These would be called 'source terms' in today's parlance. However, and this is the key point, in order to make use of the criteria, it is necessary to assess the various probabilities of different levels of release. At that time this was a difficult task because of the lack of quantitative data for failure rates of different components. This need for the acquisition of reliability data was well appreciated in the UK and led to the setting up of the Safety

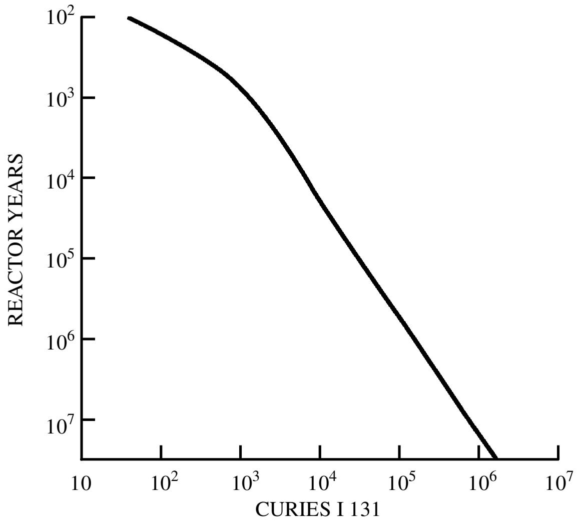

Figure 1. Criteria for release of ^{131}I proposed by Farmer in 1967. Reproduced from Reference 20 by permission of the IAEA.

and Reliability Service in the United Kingdom Atomic Energy Authority (UKAEA) in 1970. This eventually became part of the National Centre of Systems Reliability and this had, and still has, a large membership across a range of industries and from many countries. It is presently incorporated in AEA Technology, the commercial company privatized out of the 'old' UKAEA.

This database and others was an essential precursor to the complicated and detailed PSA studies which were soon to follow.

This brings us to a position in the early 1970s when the need for improved quantitative analysis was clear, and the means for it were almost all in place.

It is sometimes said that the history of PSA begins with its first major application– the *Reactor Safety Study* (WASH 1400)[21]. This introductory discussion is meant to show that whilst this is indeed the case so far as a full-scale PSA is concerned, it was made possible by the evolution of requirements for better ways of evaluating the reliability of plant, and of the consequences of the resulting releases of radioactivity.

The rest of this review follows the evolution of the full quantitative PSA method from the *Reactor Safety Study* (RSS), through a number of later defining studies (Zion, Indian Point and the Sizewell B Analysis) in Section 2, to the point where the methodology and its implications were debated in a public/legal forum– that is, the Sizewell B public enquiry. Finally, the definitive compendium document on guidance for PSA users– NUREG 1150 of 1989[22]– is used to close off this intensive period of methods development. The resulting lessons learned have contributed to its continued use, especially as a possible regulatory tool, and this is given some attention in Section 3. Then in Section 4, I review the state of the art in the methodology and highlight where the current outstanding issues are.

In Section 5 I briefly summarize the R&D which has been undertaken to back up the severe accident analysis requirements of a full-scope PSA, and indicate where we seem to be at present. Some spin-offs and practical uses of this research, particularly in accident management and in the treatment of human factors, are discussed.

Since one of the original 'visions' for PSA was in its use as a tool for judging the acceptability of plant against risk-based criteria, I include in Section 6 a brief examination of how regulatory authorities have responded to the development of this major new tool. I try to indicate why it has not been fully incorporated into the regulatory process and draw some conclusions concerning implications of the use of 'risk' as a quantitative acceptance parameter as a result of the extensive discussions of the matter at the Sizewell B public inquiry.

After the mid-late 1980s, the evolutionary path of PSA divides into many different areas and it becomes increasingly difficult to maintain a coherent overview. However, in Section 7 I consider some of these newly developed areas and, with a little crystal-gazing, try to identify clear messages for the future.

In summary, the main sections of this review are:

Section 2: Milestone PRA calculations
Section 3: Major insights gained from the studies
Section 4: The state of the art in PSA methods
Section 5: Severe accident research and development
Section 6: The regulators' views of probabilistic methods
Section 7: Summary and messages for the future

2. MILESTONE PSA CALCULATIONS

The key developments in the *methodology* of PRA came during the decade 1975–1985. A number of ground-breaking analyses were performed which have shaped the nature of the PSA tool as it is today. This section briefly identifies these analyses and indicates the particular contributions and lessons which they gave.

2.1 The Reactor Safety Study (WASH 1400)

Although it is now almost universally agreed that the RSS was *the* milestone study for PSA and that it has radically changed how active safety issues are addressed, it is a measure of the pace of development that it is now equally considered to be outdated. However, any review of PSA development should begin with at least the realization that many of the features that we now consider to be written on 'tablets of stone' were in fact invented for use in the RSS and, regardless of technical advances, remain the accepted form today. In reviewing the RSS, therefore, it is useful to highlight some of these now established aspects of PSA, through reference to their past use.

The RSS studied two LWR systems– the Pressurized-Water Reactor (PWR) at Surrey 1 and the Boiling-Water Reactor (BWR) at Peach Bottom.

The concept of accident sequences and their use both as identifiers of important nodal points in accident development and as conceptually appealing means of representing the possible outcomes was evolved in the RSS. This way of categorizing accidents is still in common use, as is the nomenclature first devised in the RSS. This is illustrated in Table 1, where the original RSS classification scheme is shown. The description of accident sequences was taken one step further by the RSS in that accidents with nominally similar fission product releases were again condensed into a smaller set of groups called release categories. Nine such categories were defined. This was a less satisfactory aspect

Table 1. Categorization and nomenclature for accident sequences. Reproduced from Reference 21 by permission of the USNRC.

Symbol	Description
A	Intermediate to large LOCA
B	Failure of electric power to ESFs
B^0	Failure to recover either on-site or off-site electric power within about 1 to 3 hours following an initiating event which is loss of off-site AC power.
C	Failure of containment spray injection systems
D	Failure of emergency core cooling injection systems
F	Failure of containment spray recirculation system
G	Failure of containment heat removal system
H	Failure of emergency core cooling recirculation system
K	Failure of reactor protection system
L	Failure of secondary relief valves and the auxiliary feedwater system
M	Failure of the secondary system steam relief valves and the power conversion system
Q	Failure of primary system relief valves to close after opening
R	Massive rupture of the RPV
S_1	A small LOAC with an equivalent diameter of 2–6 inches
S_2	A small LOCA with an equivalent tube diameter of $\frac{1}{2}$–2 inches
T	Transient event
V	LPIS check valve failure (interfacing systems LOCA)
α	Containment failure due to reactor pressure vessel steam explosion
β	Containment failure due to inadequate isolation of containment openings and seals
γ	Containment failure due to hydrogen burning
δ	Containment failure due to overpressure
ε	Containment vessel melt through

of the RSS methodology and these categories have not survived into present usage. The trend now is less toward categorization and more toward the evaluation of detailed estimates of release fractions at the accident sequence level. This is because the amounts of fission products calculated by the modern generation of computer models are found to be very sensitive to apparently small differences between sequences, and indeed for the same sequence from plant to plant[23]. To give an impression of the kinds of accident sequences which were grouped together into categories, Table 2[24] shows a breakdown of a set of release categories derived for the Sizewell B study and which I use here rather than those of the RSS as they are more descriptive and they already include additional insights.

One innovation introduced in the RSS which has become firmly established in PSA methods is the use of the CCDF (Complementary Cumulative Distribution Function)* as a means of displaying the numerical results for risk. The principal reasons for this are outlined in the RSS[21] (Main Report, 2.2, p. 11). The expression of risk as an individual risk number such as 10^{-5} per year had been used previously in attempts to delineate risk acceptance levels at that time[25]. However, the RSS authors were not satisfied with this individual risk representation since it does not differentiate with respect to the magnitude of the consequences of accidents. Society generally views the single large consequence event unfavourably compared to the total of small events having the same average risk. This is reflected in the Farmer criterion[20] which was risk averse, and indeed the authors of the RSS (notably Professor Rassmussen) have acknowledged that Farmer's approach influenced their choice of CCDFs to demonstrate aversion.

The concept of risk aversion was introduced to account for the fact that large consequence events are viewed with such horror that their low frequency is likely to be discounted when judgements concerning acceptability are to be made. It may be said that the RSS, in leading the way in showing the consequences of reactor accidents in terms of numbers of people who could be killed or the area of land which might be contaminated, did the nuclear industry a disservice. In reality, events of the past 10 years have shown that such quantification and expression of risk in meaningful terms has led to vast improvements in the industry's understanding of risk. It has also led directly to action which has reduced the risk from operating, and future, power plants.

Whether risk aversion should be considered, and at what levels of consequence the public would become concerned, is not for PSA analysts alone to pontificate upon– as a topic it is still under lively debate and is discussed further in Section 6. Here I only wish to point out that judgements concerning the acceptability or tolerability of risk can only be made if a reasonable assessment of the risk posed by a plant is available. PSA provides the means for quantifying the risk, and the RSS led the way in expressing the results in a form useful for such a purpose.

The methods developed for expression of the risks in the RSS study are illustrated in Figures 2 and 3 where CCDFs for early and delayed facilities are shown respectively. These curves indicated explicitly (for the first time) that there was a (low) chance that more than ~ 4000 people might be killed *immediately* and ~ 50,000 later as a result of a reactor accident. As an additional source of worry to the public, the RSS also gave details of the potential ground contamination as shown in Figure 4. The principal authors of the RSS believed that these figures represented such a low risk that the public would immediately recognize the logic of nuclear power as a clean and safe technology. They failed to take into account their own judgement on risk aversion and that low frequencies are much harder to comprehend than large consequences.

*CCDFs give values for the probability of exceeding certain levels of consequences.

Table 2. Description of accident release categories used in the Sizewell B PSA: (a) Category descriptions; (b) Grouping of chemical species. Reproduced from Reference 41 by permission of Westinghouse.

(a)

Release category	Summary description
UK1	Used for accident sequences involving core melting, where a containment bypass pathway from the primary circuit to the environment exists. The pathway considered in this study is the failure to the isolation valves separating the reactor cooling system and the low pressure residual heat removal system. It is equivalent to the V sequence of the RSS.
UK2	Used for overpressure failure events with a source term reflecting the possible occurrence of a steam explosion, and in which the containment sprays are not functioning. It is also used to include those sequences where, although there is no steam overpressure failure, an isolation failure or small bypass of the containment occurs.
UK3	Used for early overpressure failures where sprays are not functioning. It is also used for sequences where sprays are functional but where containment failure occurs so soon after most of the fission products are released from the reactor system that the sprays are not effective in removing fission products from the containment atmosphere and in particular for small-break sequences.
UK4	Used for overpressure events with the assumed occurrence of a steam explosion at a time when the spray system is functioning.
UK5	Used for late overpressure failures without sprays operating. Failures are as a result of relatively slow pressure build-up due to loss of containment heat removal capability. It is pessimistically assumed that failure occurs after 4 hours. Cooling of the core debris is lost so that dry-out and vaporization release occurs.
UK6	Used for late overpressure failures without sprays operating. Failures are as a result of relatively slow pressure build-up due to loss of containment heat removal capability. In this case, failure is assumed to occur after 8 hours. Debris in the cavity from the molten core remains covered by water so that no vaporization release occurs.
UK7	Used for delayed overpressure failure events following a large break LOCA with spray systems functional for a significant period before RPV failure.
UK8	Used for delayed overpressure failure sequences for which the spray systems are functional.
UK9 and 10	Used for melt-through of the base mat, with and without spray failure respectively. A release takes place through the base mat and the surrounding soil to the atmosphere.
UK11 and 12	Used for all degraded core accidents in which the containment remains intact or for which the system is recovered. UK11 and 12 refer to cases with and without spray failure, respectively. Radioactive release to the environment would be small, corresponding only to normal levels of containment leakage.

(b)

Class	Description
1	Xenon (Xe) and krypton (Kr) noble gases
2	Organic iodine
3	Elemental iodine, halogens
4	Caesium (Cs) and rubidium (Rb) alkali metals
5	Tellurium (Te)
6	Barium (Ba) and strontium (Sr) alkaline earths
7	Ruthenium (Ru) noble metals
8	Lanthanum (La) refractory oxides, including actinides.

As the first comprehensive study, the RSS clarified many of the ‘insights’ which are now generally associated with the implementation of PSA studies. Rather than repeat them, I defer the description of a list of such insights until I have discussed the contributions of other milestone studies. However, several features of the RSS results should be highlighted because they had a significant impact on the way the methodology developed post 1975.

First, the study indicated that, contrary to any preconceived notions, large pipe breaks did not dominate the risk posed by the plant. Rather the performance of valves (failure to reseat), small pipe breaks and transient events and human action all contributed significantly to the risk. No simple, single features were identified[26]. Thus, emphasis in more recent studies has been on methods for handling multiple or dependent failures (common cause failure), completeness (that is, have all possible routes/sequences been identified?) and human/machine interfaces.

Even though the RSS’s treatment of post core melt events is now considered to be rather crude, one of the most far-reaching insights gained by the study was that core melt did not always equate to very large consequences. In the RSS, following a core melt, the containment boundary was always assumed to be penetrated; this conclusion arises from the fact that basement melt-through was considered ‘unstoppable’ because of the high decay heat generated by the molten core (the so-called ‘China’ syndrome). However, this route to the environment would lead to considerable filtering of the radionuclides and thereby reduce the amount available for harm to the population. More recent thinking is that the containment is rather unlikely to fail at all. And, indeed, one question of whether Reactor Pressure Vessel (RPV) failure is an inevitable consequence of core melt (or partial core melting) has been raised by the very detailed analysis which has been completed on the physical processes underlying the TMI-2 accident sequence development[27]. However, the realization that core melt did not equate necessarily to catastrophic consequences led to the now very large programme of work investigating containment performance so that proper account may be taken of it in risk assessment. This boils down to developing data and methods to enable the performance of buildings and equipment to be evaluated when subjected to conditions beyond their design limits and in devising ‘severe accident management’ schemes aimed specifically at containing or mitigating core melt accidents[28].

A natural ramification of the realization that not all severe accidents lead to very large releases is that the most likely

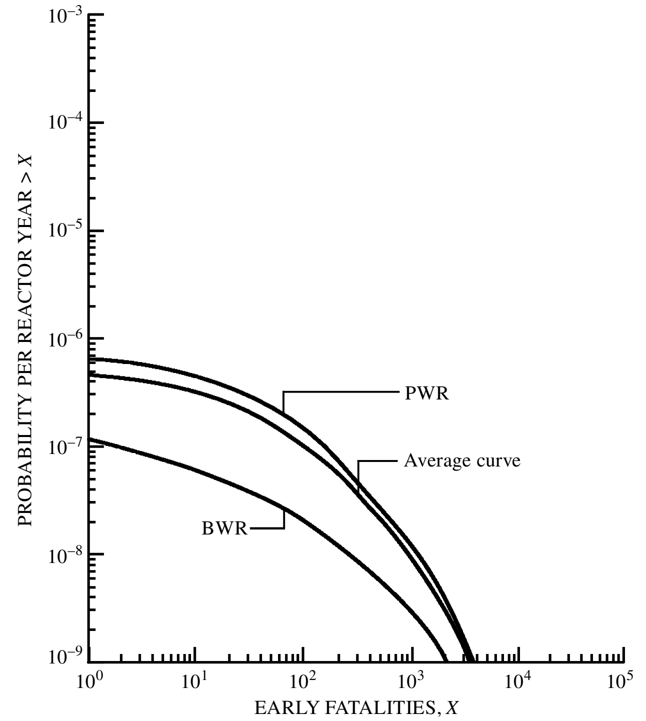

Figure 2. RSS results for risks of early fatalities per reactor year of operation for PWR and BWR plant in the form of CCDFs. (Approximate uncertainties are estimated to be represented by factors of 1/4 and 4 on consequence magnitudes and by factors of 1/5 and 5 on probabilities.) Note that as early as the RSS there was a qualitative attempt to represent uncertainties.
Reproduced from Reference 21 by permission of the USNRC.

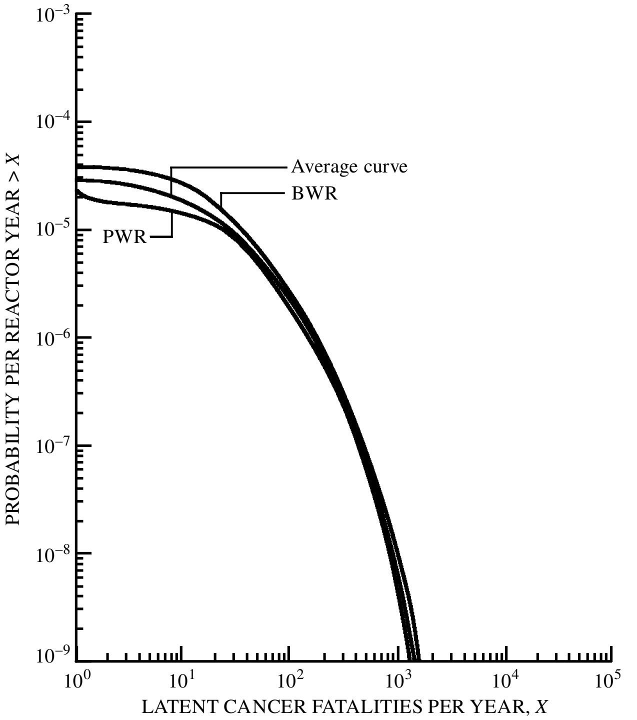

Figure 3. RSS results for risks of latent cancer fatality incidences per reactor year in the from of CCDFs. (Approximate uncertainties are estimated to be represented by factors of 1/6 and 3 on consequence magnitudes and by factors of 1/5 and 5 on probabilities.)
Reproduced from Reference 21 by permission of the USNRC.

result of a core melt accident is a very small number (if any) of off-site consequences. This may seem self-evident today, but it was not so in 1975. The RSS authors were quick to point this out and said:

> 'For the most likely course of events following the melting of the core; the number of fatalities expected is much smaller than those that commonly occur in accidents such as fires, explosions and crashes of commercial airliners.
>
> 'In addition the likelihood of core melt is calculated to be much smaller than any of the above.' [Reference 21, 1.8, p. 6]

In order to demonstrate these insights the RSS compared the calculated results, taking a reactor programme of 100 reactors, with statistical data from other activities. This is the now quite well known Figure 6-1 of the RSS and is shown here as Figure 5. Much has been said concerning the propriety of making risk comparisons of this type; this cannot be followed up here, but see References 6 and 29 for example.

In the RSS the final remarks [Reference 21, 1.10, p. 7] are:

> 'This report provides considerable background for gaining an understanding of the concepts involved in risk assessment and of the elements involved in nuclear power plant safety. The results of the study of nuclear reactor accident risks are presented and compared with risks due to natural phenomena and other technologies in our society in order to provide perspective on low probability risks. A large amount of information has been developed in conducting the study

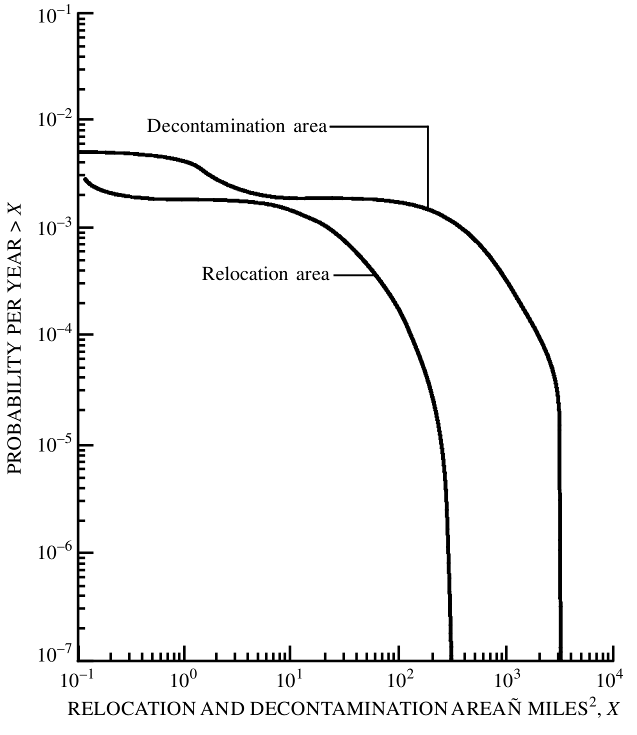

Figure 4. RSS results for probability of ground contamination following a reactor accident in the form of CCDFs. (Approximate uncertainties are estimated to be represented by factors of 1/5 and 2 on consequence magnitudes and by factors of 1/5 and 5 on probabilities.)
Reproduced from Reference 21 by permission of the USNRC.

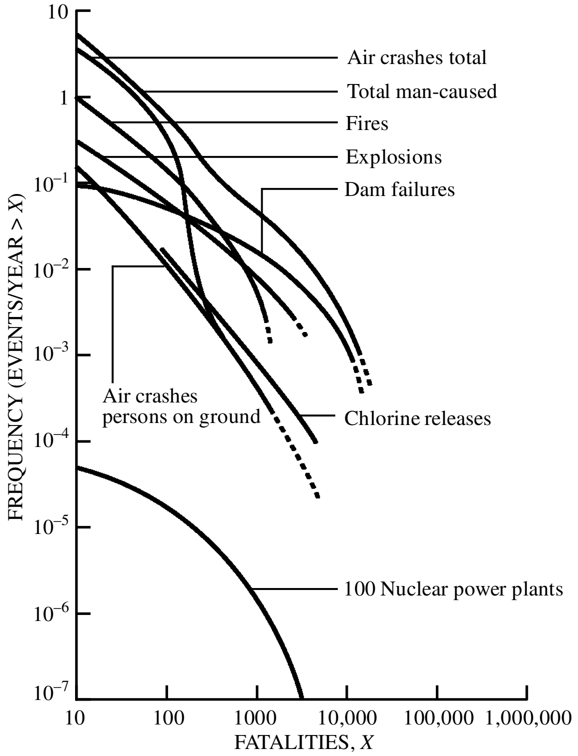

Figure 5. RSS results comparing risks (in the form of CCDFs) from 100 nuclear power stations and other industrial activities and naturally occurring events. Fatalities due to auto accidents are not shown because data are not available for large consequence accidents. Auto accidents cause about 50,000 fatalities per year.
(All of the statistical data in this figure are relevant pre-1975.)
Reproduced from Reference 21 by permission of the USNRC.

and most of it is presented in this report and its appendices. It is expected that this information will be of use in making the controversy about reactor safety more objective. Obviously, the question of the acceptability of nuclear accident risks requires a much broader social judgement that transcends the scope of the Reactor Safety Study.'

Just how successful it has been in bringing objectivity to risk assessment can be gauged from the developments since and the industry which has now developed to serve the needs of the utilities and regulators in PSA.

2.2 The Zion[30] and Indian Point Studies[31]

These studies are included here because they represent two very important milestones in the early use of PSA. First, these were the initial studies to include comprehensive and detailed assessments of the effect of a range of external events on the risk and second, it was the first time that PSA had been used in a licensing or regulatory sense. In late 1976, the US Nuclear Regulatory Commission (NRC) Commissioners, as a result of a petition to shut down the Indian Point plants, required that Zion[2] and Indian Point perform in-depth risk studies. Over three years, detailed studies investigating all aspects of external (seismic, fire, wind, flood) as well as internal risk were conducted. These were the first studies to examine seismic and fire risks, including uncertainties, in detail, and as such represented a test of the method. In addition, substantial advances were made in the evaluation of severe accident phenomenology, which included realistic transient analysis and containment strength, a detailed 'containment event tree', and supporting experimental programmes in areas of hydrogen combustion and debris bed coolability. Following review and comment by NRC contractors, this study served as a focal point in an Atomic Safety and Licensing Board (ASLB) hearing addressing the Indian Point site. In spite of the substantially higher-than-average population density, the study concluded that the risks were comparable to risks at other sites and well within the Commissioners' then-proposed safety goals[32]. An NRC sponsored study conducted at the same time investigated a broad variety of sites and PSA studies, and concluded that risk variability due to population differences is not as significant as is the risk variability due to design differences[33,34].

Even though the models for core melt progression and containment performance were considerably improved over those available to the RSS, a significant conclusion from these studies, and especially the containment analysis, was that the more we knew about core melt, the less likely that very large accident consequences would eventually arise. This led directly to the creation of a major R&D effort for better understanding of severe accidents. A brief historical overview of this important research area is given in Section 5, but note that even though those programmes have been running, in some cases, in excess of 15 years, 'closure' is, in many cases, still elusive[35].

The calculated values for the contribution to core melt from the various accident sequence types (for internally initiated events) are shown in Figures 6 and 7. These are from the Zion Study and are included to illustrate how the important contributors can be identified, both at the accident sequence level and release category level. Note that in these figures it is not total risk which is being used to determine the relative contributions. This is an important feature because the principal contributors to either a release category (a rather artificial quantity) or to core melt frequency will not necessarily have the same ranking with regard to *risk*. This is discussed more fully in the section devoted to Sizewell B below.

External events

One of the most important features of the Zion and Indian Point Studies was their comprehensive treatment of external events.

The range of external events considered included:

1. Fire
2. Floods
3. Tornadoes (and associated missiles)
4. Aircraft accidents
5. Turbine missiles
6. Transportation and hazardous materials
7. Seismic effects.

In order to show the effects of external events, results in the same format as Figures 6 and 7 are shown for Indian Point 2 and 3 in Figures 8 and 9. In these figures the contribution from external events is shown hatched. Even

[2] Note that the Zion plant, owned by Commonwealth Edison, was, in fact, closed in 1998.

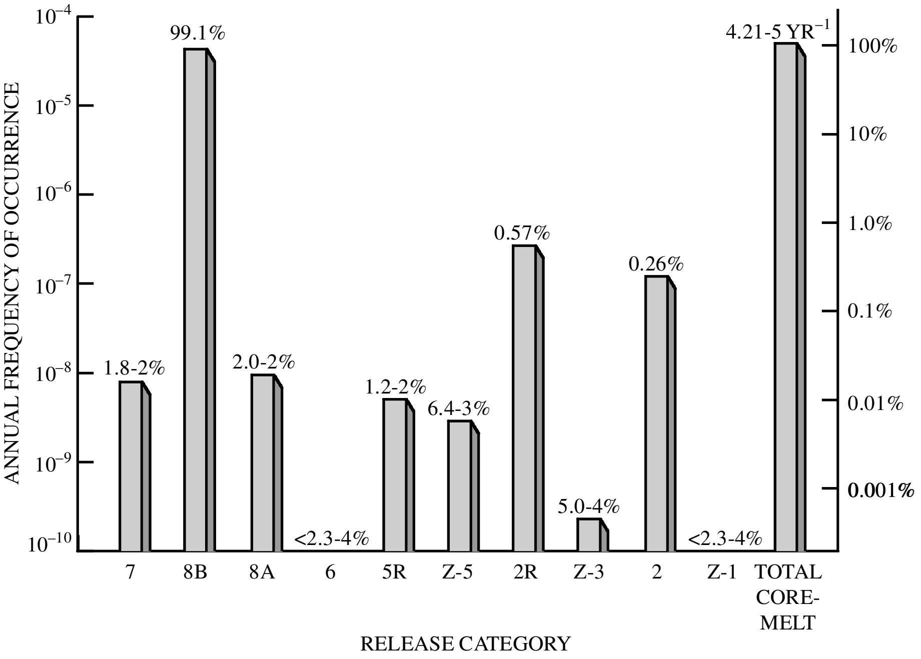

Figure 6. Zion PSA results: contribution to total core melt frequency by release category. The release category definitions are given in Reference 31, but note that the dominant category (8B) represents a very small release to atmosphere as it is for an accident sequence in which the containment remains intact and the in-containment spray system is functional. The release categories are:
Z-10– seismic failure of containment
Z-1– early overpressure failure of containment
2– containment bypass
2RW– late overpressure failure of containment
8A– containment intact without spray operation
8B– containment intact with spray operation
Reproduced from Reference 30 by permission of ComEd.

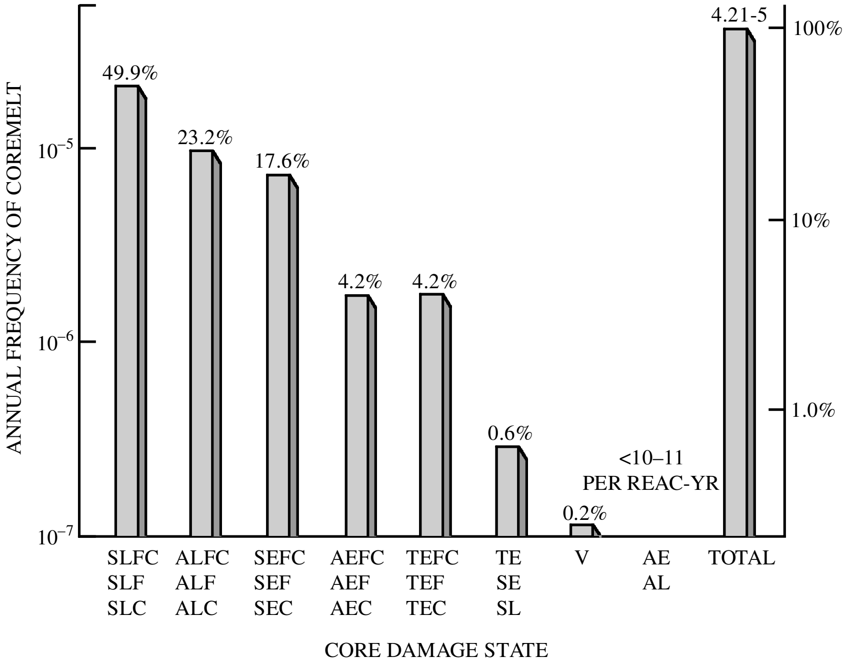

Figure 7. Zion PSA results. Contribution to total core melt frequency by core damage state. The core damage states are defined by lists of initiating and subsequent events and can be interpreted using Table 1. Thus, for example, the designation SLFC is a sequence of events comprising:
S = small LOCA
L = failure of secondary system steam
F = failure of containment spray recirculation system
C = failure of containment spray injection system
For V sequence this is LPIS check valve failure (that is, containment bypass).
Reproduced from Reference 30 by permission of ComEd.

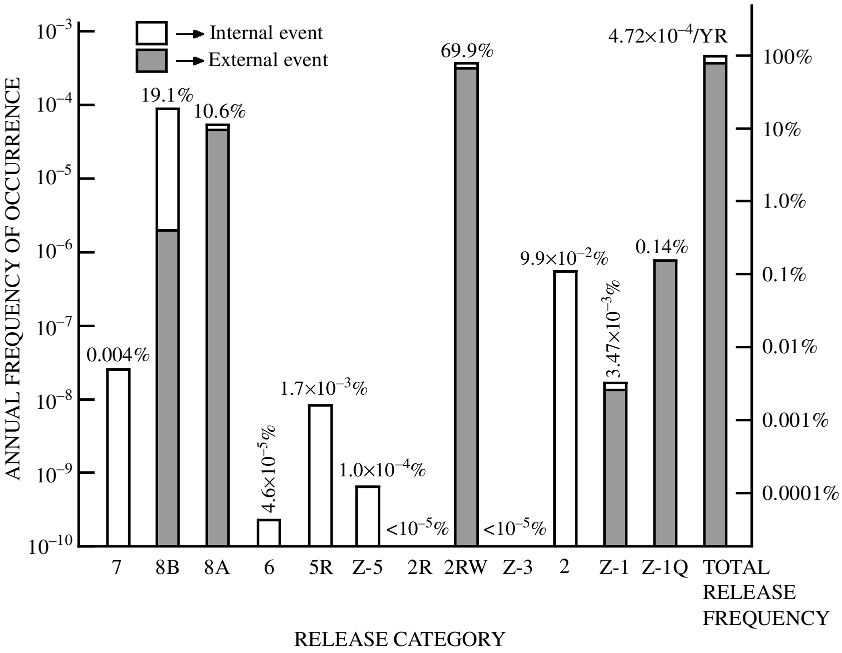

Figure 8. Indian Point PSA. Contributions to total release frequency by release category (as defined in the caption to Figure 6.) highlighting the contributions from internal and external events.
Reproduced from Reference 31 by permission of Consolidated Edison Co.

though both Zion (for which similar results were obtained) and Indian Point are in areas thought to be relatively 'safe' *vis-à-vis* external hazards, the contribution to core melt frequency is ⩾50% overall from these events. Clearly, if internal initiators are reduced, then eventually the very large but very low probability external events must dominate the total risk and may well represent an ultimate level of risk attainable for the technology. Table 3 gives the detailed breakdown of results in tabular form. This is taken from Tables 8.3-2A-1 and 8.3-2A-1 (revised)[33].

A representative calculated risk curve for the Indian Point 2 study is shown in Figure 10. In this the internal and external contributions to risk are shown along with the internal ones alone. The importance of external events is highlighted by this figure.

Figure 10 also gives uncertainty estimates at the 50% and 90% confidence levels. In fact, the uncertainty calculations were very much more sophisticated than might be assumed from Figure 10 and so in Figure 11 the calculated probability densities are shown for the contributions to core melt frequency for the various release categories for Indian Point 2 (see Reference 33).

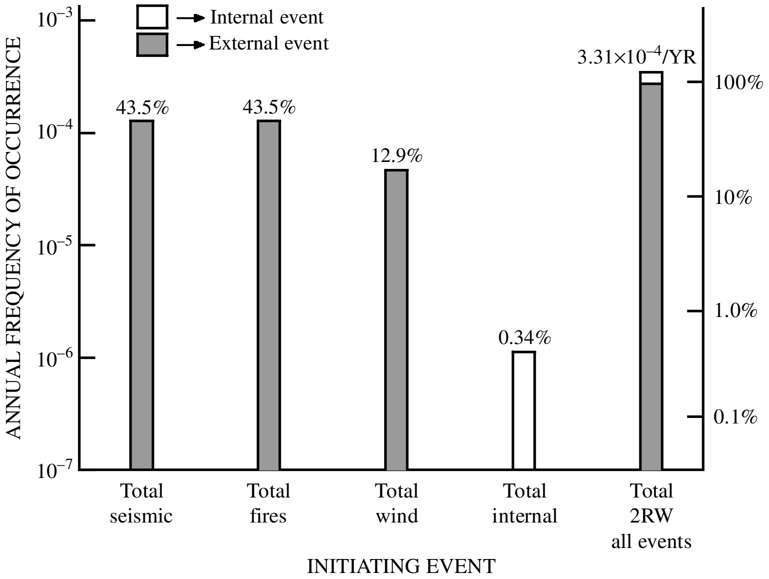

Figure 9. Indian Point PSA. Breakdown of contributions to the dominant release category in Figure 8 (2RW). The category is clearly seen as being dominated by external events, with seismic and fires contributing about equally.
Reproduced from Reference 31 by permission of Consolidated Edison Co.

Table 3. Indian Point PSA results. Contributions to total care melt frequency from internal and external events. Detailed breakdown by initiating event and release category. Reproduced from Reference 31 by permission of Consolidated Edison Co.

		Seismic failure of containment	Early overpressure failure	Containment bypass	Late overpressure	Containment intact without spray	Containment intact with spray	Total core melt
Initiating events	Release category	Z-1Q	Z-1	2	2RW	8A	8B	CM
Large LOCA (1)		0	1.6–9	1.6–9	1.8–17	1.4–9	1.6–5	1.6–5
Medium LOCA (2)		0	1.6–9	1.3–9	1.6–17	1.1–9	1.3–5	1.3–5
Small LOCA (3)		0	3.4–14	1.7–9	1.5–8	4.9–9	1.7–5	1.7–5
Steam generator tube rupture (4)		0	4.9–14	1.6–11	2.2–8	4.7–11	1.2–7	1.4–7
Steam break inside containment (5)		0	7.4–17	2.0–11	3.2–11	2.6–11	2.0–7	2.0–7
Steam break outside containment (6)		0	7.4–17	2.0–11	3.2–11	2.6–11	2.0–7	2.0–7
Loss of main feedwater (7)		0	5.8–14	1.8–10	2.6–8	3.4–10	1.8–6	1.8–6
Loss of one MSIV (8)		0	1.1–14	1.8–11	4.9–9	5.1–11	1.7–7	1.7–7
Loss of RCS flow (9)		0	1.1–15	3.3–12	4.8–10	6.2–12	3.2–8	3.3–8
Core power excursion (10)		0	6.7–23	2.1–19	3.0–17	4.0–19	2.0–15	2.1–15
Turbine trip (11a)		0	6.3–14	2.0–10	2.9–8	3.7–10	1.9–6	2.0–6
Turbine trip, loss of offsite power (11b)		0	2.2–12	3.9–9	1.0–6	3.5–9	3.7–5	3.8–5
Turbine trip, loss of service water (11c)		0	7.8–15	6.4–12	3.5–9	3.6–13	5.7–8	6.0–8
Reactor trip (12a)		0	5.9–14	9.8–11	2.7–8	2.8–10	9.3–7	9.6–7
Reactor trip, loss of component cooling (12b)		0	1.7–17	3.7–12	7.7–12	3.1–12	3.7–8	3.7–8
Interfacing system LOCA (V)		0	0	4.6–7	0	0	0	4.6–7
Switchgear room		0	0	0	5.6–5	0	0	5.6–5
Electrical tunnel		0	0	0	8.8–5	4.8–5	0	1.4–4
Cable spreading room		0	0	0	3.0–7	0	1.6–6	1.9–6
Diesel generator building		0	0	0	4.4–8	0	4.0–7	9.0–7
Tornado		0	0	0	1.6–5	4.9–10	0	1.6–5
Hurricane		0	0	0	2.7–5	0	0	2.7–5
Total seismic		6.8–7	1.3–8	2.9–8	1.4–4	4.2–9	2.6–10	1.4–4
Total wind		0	8.5–11	8.5–9	4.3–5	4.9–10	0	4.3–5
Total fires		0	3.0–10	3.8–8	1.4–4	4.8–5	2.5–6	2.0–4
Total internal		0	3.2–9	4.7–7	1.1–6	1.2–8	8.8–5	9.0–5
Total all events		6.8–7	1.7–8	5.4–7	3.3–4	4.8–5	9.1–5	4.7–4

Note: 1.6–9 is read as 1.6×10^{-9}.

The indication of 'fire' as a serious and significant accident initiator is borne out by experience. The fire at the TVA Browns Ferry Plant was a very near miss, and more recently, the most likely initiator for severe accidents in Russian-designed plant has been identified as from internal fires. (See, for example, Reference 36.)

2.3 Major PSA Studies on Reactors at the Design Stage

It is a moot point as to whether PSA as currently available could be described as a 'design tool'. However, it is clear that the PSA performed by Westinghouse and UKAEA staff for the proposed Sizewell B PWR was done at the design stage and may be legitimately seen as having had an influence on the design. (For an authoritative description of how the then CEGB viewed the use of PSA for the Sizewell Study, see Reference 37.)

The rationale for performing a PSA at an early stage of the design process has been described in the proof of R R Mathews (CEGB's safety director at the time) (CEGB P2)[37] and in the CEGB's statement of case[38] to the Sizewell B Public Inquiry. In Chapter 21 (paragraph 21.3) it is stated that:

'The design targets are set at levels of probability so low that, if they are met, the chances of failing to cope satisfactorily with any postulated accident are very remote. It might be considered unrealistic to try to go further and anticipate what would happen if all of the safety provisions failed completely. The CEGB has nevertheless initiated studies which do attempt to analyse those very remote possibilities. It has done so for a number of reasons. First, it requires confirmation that the predicted probabilities of very severe accidents occurring are not immediately below the criterion or 'cut-off' point for design basis accidents. If this were not confirmed, then some alternations in design could be required to reduce the probability to a new, lower, level. Secondly, the CEGB feels that it is desirable to understand the potential consequences of uncontrolled releases; this provides a measure of the possible harm which could result from such accidents against which to balance the large resource, cost and effort that is expended to ensure the

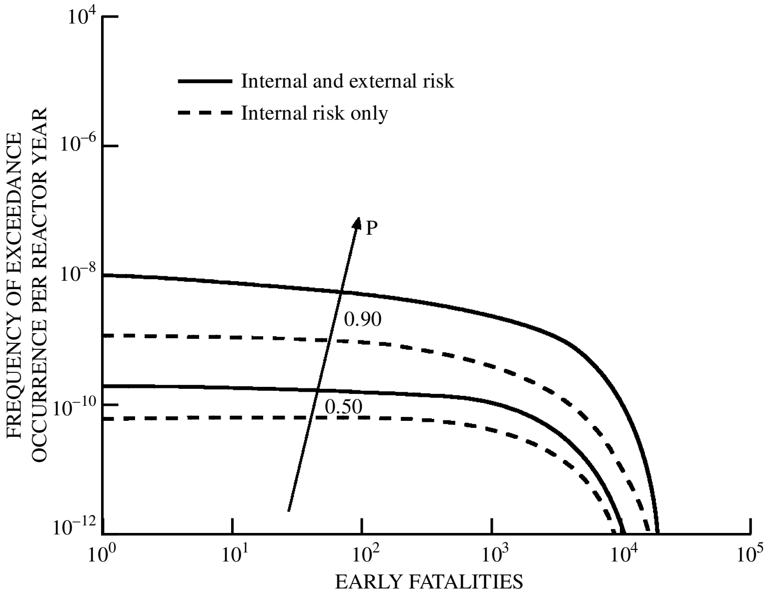

Figure 10. Internal and external CCDFs compared to internal risk only for the Zion study. Reproduced from Reference 30 by permission of ComEd.

safety of nuclear plant. The accident at Three Mile Island has led to an intensification of efforts on the analysis of events which could lead to a degraded core.'

Since the Sizewell B Public Inquiry did not form part of the formal licensing process, it cannot be said that the PSA was performed with the Nuclear Installations Inspectorate (NII) in mind. However, it is clear that the NII would wish to have such a study available, and it has said so[39]. The NII's need is to be provided with an assurance that no accident with very severe consequences is likely at a frequency only just below the design basis– that is, that there is no 'cliff edge' in the design.

The benefits of performing PSA calculations at an early stage in the design process are clear. Even when the methodology was still evolving, its usefulness had been noted and implemented by the reactor designers. The comments[40] of D.C. Richardson (Westinghouse Corporation) who acted as manager for much of the Sizewell B degraded core study[41] gave a clear indication of that. In passing, note that few, if any, of the insights quoted here depend upon the consequence (that is, risk) assessment aspects of PSA. This point will be returned to.

The results of the Sizewell B study are given in Proof 16 (Degraded Core Analysis– J. H. Gittus[42]) and in addenda, particularly Addendum 3, which contains revised results. The results used here are taken from the December 1983 version of P16 Addendum 3. Table 4 gives the collected

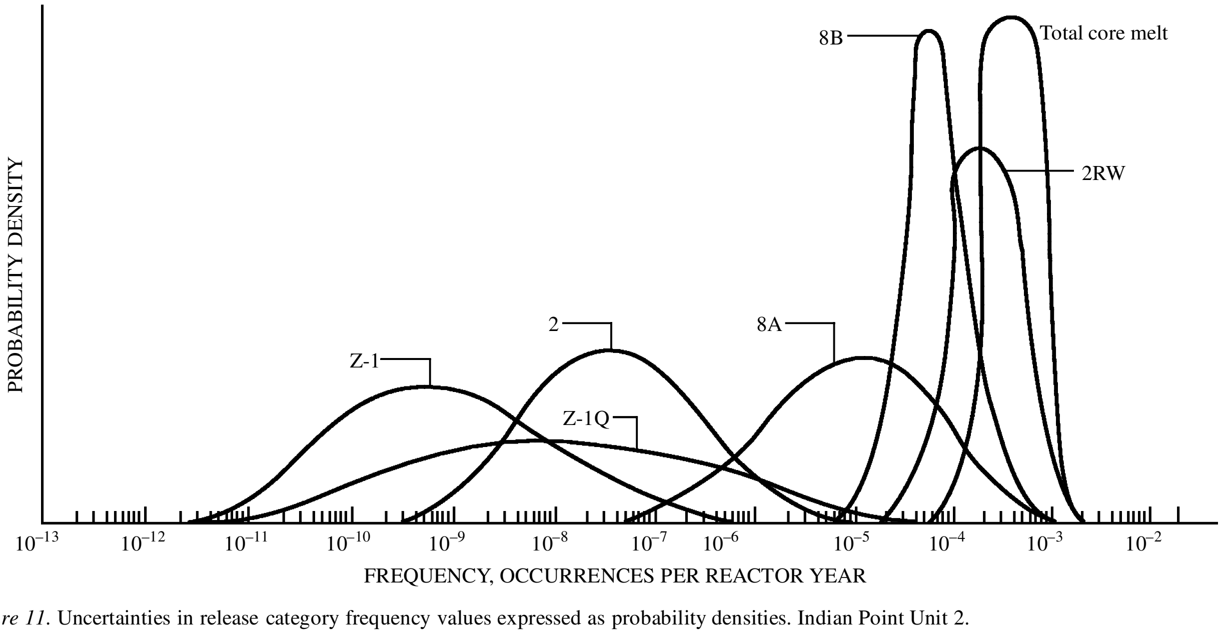

Figure 11. Uncertainties in release category frequency values expressed as probability densities. Indian Point Unit 2. Reproduced from Reference 31 by permission of Consolidated Edison Co.

Table 4. Frequencies of risk important sequences from the Sizewell B PSA. Note that the ranking with regard to frequency of significant release is not at all correlated with the contributions of the sequences to core melt frequency. Reproduced from Reference 41 by permission of Westinghouse.

Rack with respect to degraded core frequency	Sequences	Frequency of degraded core, per reactor year of operation	Percentages of total degraded core frequency	Conditional probability of containment failure or bypass	Frequency of significant release, per reactor year of operation	Relative rank with respect to frequency of significant release
1	Small LOCA coexistent with loss of component cooling	2.85×10^{-7}	23.0	2.65×10^{-2}	7.55×10^{-9}	3
2	ATWT coexistent with turbine trip failure	1.35×10^{-7}	10.9	2.65×10^{-2}	3.58×10^{-9}	4
3	Large LOCA coexistent with loss of component cooling	1.03×10^{-7}	8.3	1.21×10^{-2}	1.25×10^{-9}	8
4	Medium LOCA coexistent with loss of component cooling	1.03×10^{-7}	8.3	1.21×10^{-2}	1.25×10^{-9}	8
5	LOCA beyond the capacity of the ECC5	1.00×10^{-7}	8.1	1.21×10^{-2}	1.21×10^{-9}	10
6	Small LOCA coexistent with failure of high head injection	9.42×10^{-6}	7.6	2.65×10^{-2}	2.50×10^{-9}	6
7	Medium LOCA coexistent with failure of high head injection	9.38×10^{-8}	7.6	1.21×10^{-2}	1.13×10^{-9}	11
8	Small LOCA coexistent with failure of recirculation	5.56×10^{-8}	4.5	3.8×10^{-3}	2.11×10^{-10}	
9	Large LOCA coexistent with failure of recirculation	5.53×10^{-8}	4.5	1.28×10^{-2}	7.08×10^{-10}	
10	Medium LOCA coexistent with failure of recirculation	5.53×10^{-8}	4.5	1.28×10^{-2}	7.06×10^{-10}	
11	Loss of steam outside containment coexistent with main steam isolation failure: excessive cooldown and rupture of vessel	3.23×10^{-8}	2.6	1.21×10^{-2}	3.91×10^{-10}	
12	Interfacing systems LOCA	2.69×10^{-9}	2.2	1.00	2.69×10^{-9}	1
13	Large LOCA coexistent with failure of low pressure injection	1.31×10^{-9}	1.1	1.21×10^{-2}	1.59×10^{-10}	
14	Loss of steam inside containment coexistent with main steam isolation failure: excessive cooldown of vessel and rupture	1.31×10^{-8}	1.1	1.21×10^{-2}	1.59×10^{-10}	
15	Loss of feedwater flow coexistent with loss of component cooling and auxiliary feedwater	1.05×10^{-8}	0.8	2.65×10^{-2}	2.78×10^{-10}	
16	Leakage to secondary coolant coexistent with failure of operator to depressurize primary circuit	1.03×10^{-9}	0.8	1.00	1.03×10^{-9}	2
–	Loss of off-site power coexistent with partial loss of emergency power and loss of component cooling	3.69×10^{-9}	0.3	8.55×10^{-1}	3.15×10^{-9}	5
–	Small LOCA coexistent with loss of off-site and emergency power	2.86×10^{-9}	0.2	8.55×10^{-1}	2.45×10^{-9}	7
–	Leakage to secondary coolant involving multiple tube rupture coexistent with failure of operator to despressurize primary circuit	2.50×10^{-9}	0.2	1.0	2.50×10^{-9}	6
			96.6			

Note 1: Significant is used in this table to indicate a release from a failed or bypassed containment.

frequencies for the risk important accident sequences. As noted in the comments on the Zion and Indian Point Studies, the sequences which rank highest with respect to core melt (here taken as synonymous with degraded core) frequency do not necessarily rank highest with respect to risk. This is shown very clearly here where the dominant contributor to core melt frequency is the small Loss of Coolant Accident (LOCA), with ~ 23% of the total core melt frequency, whilst the dominant contributor to *risk* is the interfacing systems LOCA. The latter only ranks 12 with respect to core melt frequency. The reasons are that the V sequence (interfacing LOCA) by definition involves containment bypass whereas for the small LOCA induced core melt to have the same effect an almost simultaneous above-ground failure of the containment is needed. It was calculated that only 1 in 40 core melt events would result in the failure or bypass of containment. This re-emphasizes the now perceived importance of containment survivability which was first highlighted in the RSS.

From the point of view of public risk, preventing large airborne releases offers the obvious way of mitigating the consequences of core melt accidents. Thus procedures highlighting accident management, or the provision of specially engineered safeguards designed specifically for severe accidents, have been subject to intensive studies in the decade following these initial PSAs. However, all things are relative and a balance is required between defence against extremely rare events and action for much more likely events, but having lower consequences. Thus, the financial risk to a utility from, for example, the Three Mile Island accidents, may dominate over rarer events. PSA is a tool which can help in providing a means of examining the priorities to be placed in assessing the overall risk from the plant.

Figure 12 shows the overall CCDFs for the Sizewell B analysis, with the individual release category contributions also shown. The dominance of UK1 (the V sequence) is clearly seen and reflects the ordering shown in Table 4.

Since this time (the late 1980s), virtually all 'new' designs have had PSAs performed on them, at least to level 1, and other established designs have had PSAs 'back fitted' to them. These include 'advanced' designs such as the Westinghouse AP600, ABB Combustion Engineering's System 80+, GE's ABWR and the EPR[43], to name but a few. Also, some more exotic designs such as the Swedish 'PIUS'[44], the Safe Integral Reactor SIR^{TM}[45] and the 'Mars' design[46] have had PSAs performed to establish the focal points in systems reliance on, for example, passive features[47]. I comment on these developments in Section 7. There have also been many analyses of existing plant that I am not able to discuss in detail here. These include important studies from the European point of view such as the 'German Risk Study'[48] and the PSA on the 'Standard French 900MW(e) PWR,[49]. These too have contributed to the general development of the methods and in the understanding of their applicability.

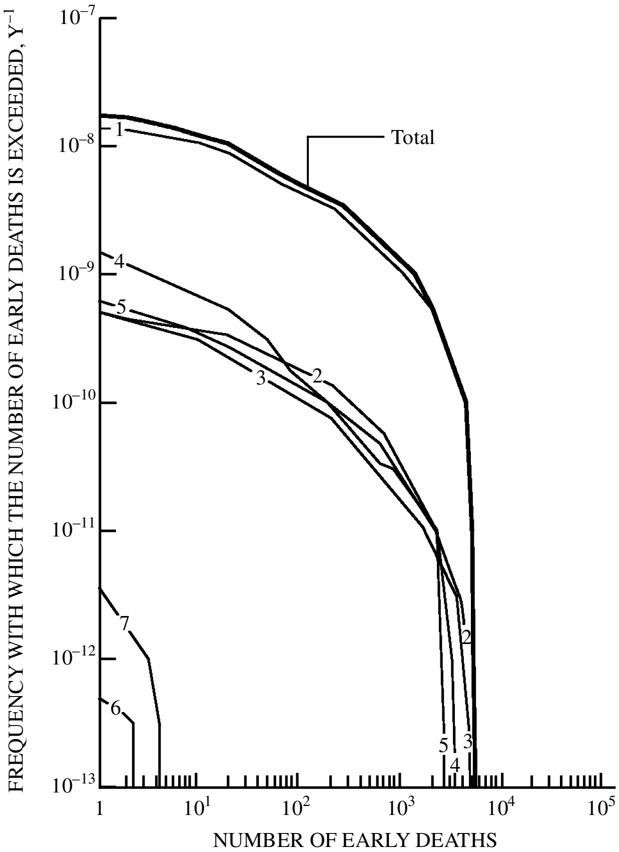

Figure 12. The Sizewell B PSA. The calculated CCDFs for early fatalities. The individual curves are for the accident sequences identified in Table 5 and follows the ranking order– that is, 1 = V sequence etc.
Reproduced from Reference 42 Crown copyright is reproduced with the permission of the Controller of Her Majesty's Stationery Office.

3. MAJOR INSIGHTS GAINED FROM THE STUDIES

From the 20 or so PSAs completed by the mid-1980s it is possible to draw a set of wide-ranging conclusions regarding the insights which may be claimed to have been established by them. The main insights from the principal studies are summarized in Table 5, which is adapted from References 22 and 41. Each individual study provided both a contribution to the overall insights, and detailed insights applicable to the specific design. It would not be realistic to ry to identify very design-specific items, even if such information were generally available. Utilities, especially in the USA, tend to be guarded about releasing specific information on their plant because of possible litigation. In the next section I consider application to *generic* plant components and these give a reasonable overview of the kind of detailed, plant-specific results which can be obtained.

3.1 Global Insights

In addition to plant-specific and generic insights, the PSAs performed to date have yielded certain global insights that it is believed apply not only to the plants analysed but to all or most current nuclear power plants, based on our knowledge of their general design and operating characteriztics. These, in some instances, apply to quite disparate reactor types (for example, Liquid Metal cooled Fast Breeder (LMFBRs) or High Temperature Reactors (HTRs)) but remember that the PSA applications in this review have been dominated by LWR studies and this will necessarily bias the trends.

The process of performing PSA studies yields extremely valuable engineering and safety insights. Conceptual insights are the most important benefits of PSAs, and the most general of these is the entirely new way of thinking about reactor safety in a logic structure that transcends normal design practices and regulatory processes. PSA methods introduce much-needed realism into safety evaluations in contrast with more traditional licensing analyses that generally use a conservative, qualitative approach that can mask important safety issues.

The estimated frequency of core melt is generally higher than had been thought before the RSS. However, unlike the RSS, most core melts are not expected to result in large off-site consequences. The small fraction of accidents that might lead to large off-site consequences generally involve either an early failure of the containment in relation to the time of core melt, or a containment bypass. For other containment response modes, the retention properties of the containment are substantial. Lack of a significant containment function is now considered to be one of the most damning criticisms of early versions of the Russian designed RBMK and VVER 440 230 reactors.

The range of core-damage-frequency point estimates in the library of PSAs used here (Table 5) covers about two orders of magnitude ($<10^{-5}$ to 10^{-3} per year). An examination of variability in the results indicates that quantitatively pinpointing reasons for the differences is extremely difficult. It is possible, however, to uncover general reasons for the variability that are attributable to plant design, operation, site characteriztics, scope of the studies, PSA methods employed and analytical assumptions postulated. Caution must be exercised in comparing the quantitative results of various PSAs, if they were produced by different teams, using different databases and perhaps even methods. In general, internal comparisons offer the most beneficial use of PSA results for practical applications.

The specifics of dominant accident sequences and the estimates of risk vary significantly from plant to plant, even though each plant meets all applicable regulatory requirements of the host country.

The following global insights about off-site consequences have been identified:

- Estimated risks of early fatalities and injuries are very sensitive to source-term magnitudes, the timing of releases and assumptions about the effectiveness of emergency plans.
- Estimates of early health effects differ greatly from one site to another, but site-to-site differences are substantially less for latent cancers.
- Airborne pathways are much more important than liquid pathways.

Accidents beyond the design basis (including externally initiated events) are the principal contributors to public risk. This indicates that the designers, operators and regulators have been generally effective in reducing the risks from expected operational occurrences and design basis accidents.

PSA studies have provided a diverse assessment of the ways in which various elements of reactor safety contribute to risk when compared to traditional safety analysis. Among the principal insights are the following:

- Human interactions are extremely important contributors to safety and reliability of the plants. This includes all types of interactions that humans can have, either with a system or with other humans, that can impact the frequency or consequences of an accident sequence.
- Test and maintenance considerations are important contributions to safety and reliability of the plants.
- Dependent and common cause failures are important contributors to plant risk.

The failure of long-term decay heat removal is a major functional contributor to core-melt frequency.

Small LOCAs and transients are dominant contributors to core-melt frequency in most PSAs, while large LOCAs are usually not. This, of course, is a very much PWR-oriented conclusion.

Earthquakes, internal fires and floods seem to play an important role in plant risk, although this tentative conclusion appears to be highly plant and site specific.

Whilst much attention has been placed on dominant accident sequences and ways to reduce risk even further, one of the most important insights gained from PSAs is the need to identify and maintain the reliability of risk-important systems and components at or near the levels now present. Degradation of such systems or components can sharply increase risk or the likelihood of core melt. The question of ageing plant is one receiving much attention at present. The implications for PSA, and indeed the priorities for operators and regulators, are discussed in more detail in Sections 6 and 7.

The results of a number of studies, including those used for illustration in Section 2, indicate important distinctions

Table 5. Compendium of results from PSAs performed up to ~ 1985. Reproduced from References 22 and 41 by permission of the USNRC and Westinghouse.

						Individual risk within 1 mile		
	PRA	NSSS/AE	Date/power (Mwe)	F core melt[1,2]	F major release[1,3]	Early fatality[1,4]	Cancer fatality[1,5]	Comments
Arkansas Nuclear One-1	IREP	B&W/Bechtel	1981 836	5×10^{-5}	2×10^{-5}	6×10^{-7}	2×10^{-7}	All-PWR 2[8]
Biblis B	German RSS	FRG(W)	1978 1300	4×10^{-5}	1×10^{-6}	3×10^{-8}	2×10^{-8}	Containment stronger and larger than U.S.
Big Rock Point[6]	Wood-Leaver/SA1	GE/Bechtel	1981 71	1×10^{-3}	0	0	–	Low power level, remote siting.[9]
Browns Ferry	IREP	GE/TVA (BWR/4, Mark I)	1981 1067	2×10^{-4}	4×10^{-5}	2×10^{-7}	1×10^{-6}	ATWS and interdependency in redundant RHR trains dominate core melt[10]
Calvert Cliffs	RSSMAP	CE/Bechtel	1982 850	2×10^{-3}	1×10^{-4}	9×10^{-6}	2×10^{-5}	More comprehensive IREP study in progress. AFWS redesign will lower risk and core melt frequency[11]
Crystal River	IREP	B&W/Gilbert	1980 825	4×10^{-4}	2×10^{-4}	3×10^{-6}	2×10^{-6}	P core melt reduced by factor of 3 by procedure changes[12]
Grand Gulf	RSSMAP	GE/Bechtel (BWR/6, Mark III)	1981 1250	4×10^{-5}	4×10^{-5}	1×10^{-7}	1×10^{-7}	Containment always fails directly to atmosphere, does not assume staffs analysis of ATWS risk
Indian Point-2[6]	PLG	W/UE&C	1982 873	4×10^{-4}	3×10^{-4}	3×10^{-8}	1×10^{-8}	Includes external events[7,13]
Indian Point 3[6]	PLG	W/UE&C	1982 965	9×10^{-5}	3×10^{-5}	1×10^{-9}	3×10^{-10}	Includes external events[7]
Limerick[6]	SAI	GE/Bechtel (BWR/4, Mark II)	1981 1055	2×10^{-5}	3×10^{-6}	1×10^{-8}	1×10^{-8}	Mean value, assumes ATWS fix
Millstone-1	IREP	GE/Ebasco	1982 652	3×10^{-4}	1×10^{-4}	1×10^{-7}	6×10^{-7}	Major release is in release category 3
Oconee	RSSMAP	B&W/Bechtel	1980 860	8×10^{-5}	4×10^{-5}	2×10^{-7}	1×10^{-7}	1/4-PWR 2; 3/4-PWR 3
Peach Bottom	Wash-1400	GE/Bechtel (BWR/4, Mark I)	1975 1065	3×10^{-5}	7×10^{-6}	4×10^{-8}	3×10^{-8}	Staff's analysis of ATWS would likely result in risk exceeding safety goal
Sequoyah	RSSMAP	W-1C/TVA	1978 1148	6×10^{-5}	4×10^{-5}	1×10^{-6}	5×10^{-7}	Hydrogen control reduces risk by 2 to 3
Surry	Wash-1400	W/S&W	1975 775	6×10^{-5}	1×10^{-5}	2×10^{-7}	1×10^{-7}	2/3-PWR 2; 1/3-PWR 3
Zion[6]	PLG	W/S&L	1981 1100	4×10^{-5}	4×10^{-6}	2×10^{-8}	1×10^{-8}	Includes external events
Sizewell-B	*W*+UK	*W*	1982 1340	1×10^{-6}	2×10^{-8}	2×10^{-10}	6×10^{-11}	Excludes external events.

There are large uncertainties associated with the values presented in this table. Also, PRAs were not performed using consistent methodology and assumptions.

[1] All numbers are median values or point estimates from internal initiators unless otherwise specified.

[2] Frequency of core melt 1×10^{-4} is the safety goal value for accident probability comparison.

[3] Frequency of release with potential for early fatalities assuming nominal evacuation and warning times (RSS).

[4] 5×10^{-7} is the safety goal for early fatality risk comparison. Same assumptions as 3 above unless specified.

[5] 2×10^{-6} is the safety goal for cancer fatality risk comparison. Same assumptions as 3 above unless specified.

[6] Utility-performed PRAs. All values are rough estimates based upon initial interpretation of results.

[7] Optimistic emergency response assumptions (1-hour delay with at least 8-hour warning) for dominant sequence when determining individual risk.

[8] Predicted risk is dominated by small locas and transients. Source term reduction expected to reduce predicted risk to within guidelines. Likelihood of major release could be reduced by adding parallel valves at the discharge of the boarated water storage tank or by improving DC power redundancy.

[9] Low power level (71 Mwe) results in low individual risk. Extensive design modifications necessary to reduce core melt frequency.

[10] Reduction of core melt frequency would require redesign of the residual heat removal system to eliminate commonalities between trains which reduce the significance of multiple redundancy.

[11] AFWS redesign is expected to significantly reduce core melt frequency and individual risk. IREP study including improved AFWS design will be available in spring 1983. Modifications to DW power system and engineered safety system actuation system may be required to lower core melt frequency within guidelines. Predicted risk is dominated by transient event and should be significantly reduced by new source term data.

[12] Core melt frequency could be reduced to less than guidelines levels by improving written procedures and improving the reliability of the steam supply to the EFWS turbine-driven pump. Predicted risk is dominated by small loca events. New source term information is expected to result in a moderate reduction in predicted risk.

[13] Core melt frequency is dominated by seismic considerations.

[14] Core melt frequency could be reduced to below guideline levels by redesigning the emergency AC power system to reduce dependency on the gas turbine and improving procedures for responding to transients. Predicted risk is dominated by transient events. New source term information should result in a significant reduction.

between contributors to different types of outcomes of potential accidents. The risk cannot be measured in terms of any single indicator, and changes in plant configuration that significantly affect one indicator may or may not affect the others. For example, a modification that reduces the frequency of core melt may not significantly affect public risk, and vice versa. Hence, a risk management strategy that focuses on core-melt frequency is not likely to result in the same set of actions as a strategy that focuses on public risk.

4. THE STATE OF THE ART IN PSA METHODS

It is important to recognize that the level of development and understanding varies among the different parts of the PSA. Thus, the reliance placed on PSA insights discussed in the previous section should depend upon the strength of those areas of PSA used to obtain them. The different areas have each reached a different level of development, or state of the art. This section summarizes the state of the art for all the areas that make up a complete PSA; a more extensive discussion is given in the references.

4.1 Level of Development

A PSA study is multidisciplinary. Depending on its scope, a PSA may require analyses of plant systems, human behaviour, the progression of core-melt accidents, radionuclide behaviour, health effects and seismic hazards. However, not all areas of analysis involved have reached the same level of development. For example, the methods of reliability analysis have been used in some form since World War II, whereas the methods used for analysing core-melt progression are new[21] and unique to reactor technology.

The use of PSA in the regulatory process should consider what parts of the PSA exhibit the greatest strengths and what parts may be weaker (I return to this point in Section 6). A particular area of analysis can be characterized by its degree of validity or realism, stability and need for improvement.

The fact that improvement is needed in an area raises the related question of the feasibility of achieving significant progress in that area in the next few years. I touch on anticipated future development in Section 7.

The degree of validity or realism of a method refers to the extent that approximations or conservatisms may have been knowingly or unknowingly introduced. This may have been done because of insufficient knowledge or because of the need to simplify the model. Validity is a measure of how closely the model represents actual reality. In some cases, there is so little experience with the phenomena of interest that it is difficult to reach a definite conclusion on the validity of a model. The uncertainty associated with a result may reflect inherent variation in the data base, questions about the validity of the model, or both.

Stability is a measure of the rate of change of the analysis methods in an area. If no significant changes in the methods have appeared recently, and if the methods in use are generally accepted by most of the experts in the area, the analysis area may be termed stable. This implies a certain degree of reproducibility. That is, for a stable area, different analysts working separately on a given problem will produce comparable results by similar or equivalent methods. Note that stability does not necessarily imply validity. A method may be recognized as using quite imperfect models in certain areas, yet because of the complexity of the problem there has been little progress, so the method has remained stable. The recognized need for improvement in an area is an indication that there is no overall satisfaction with the methods and this depends on our perception of the state of technology in that area. These perceptions are subject to change. For example, several years after the RSS there was little dissatisfaction with, or interest in, the area of radionuclide release, transport, and deposition after severe core damage or melting. As a result of measurements made at Three Mile Island after the accident and ongoing research, it was recognized that some of the conservative assumptions might not be appropriate and the need for improvement in this area changed accordingly[51]. Section 5 looks at how a comprehensive research programme has evolved to improve PSA methods. Each of the key sub-topics of PSA are now discussed in a little more detail.

4.2 Plant Analysis

System modelling in PSA studies is usually considered to have reached a high level of development. The degree of validity is fairly high, and recent improvements have mostly been in the areas of further automation and increased ability to treat large and complex systems. The areas needing the most improvement are human interactions and dependent failures. The data base is also weak in certain places. The techniques of fault and event trees have advanced considerably since their initial application to a full nuclear plant in the RSS and a variety of approaches to their use is available. Many sophisticated software packages are now available to perform this level of analysis. The insights drawn from system modelling are generally quite solid, even though issues about the completeness of the analysis persist.

The treatment of the underlying assumptions in system analysis (for example, success criteria, time dependencies, thermal hydraulics phenomena) is still open to debate. The transient initiator data base has improved substantially but improvements are still desirable in the failure rate data base, since the ranges (and error factors) are quite broad for some important areas. Progress has been made recently in the collection and analysis of component data, but more is needed. Few analyses of LOCA initiators are available and causal data are sparse. Thus, the overall understanding of the root causes of failure has not improved substantially. This also affects the ability to model dependent or common cause failures and quantitative efforts in this area remain largely unsuccessful. The improvements in data have not changed the insights gained from analyses very much. It is also believed that the conservatisms and the simplification in the modelling do not have a strong influence on these insights.

The modelling of human interactions introduces substantial uncertainty. This is particularly true of operator errors of commission and errors originating in misdiagnosis of accident conditions. However, even in the area of errors caused by failure to follow existing procedures, the uncertainties are of the same order of magnitude as those associated with component failure data. Progress has been made recently in this difficult area and much more work is now under way[52]. This aspect of system modelling is becoming more systematic and the results more reproducible. Recent reviews are available[28,29].

In summary, the whole area of PSA system modelling has advanced a good deal since the RSS, particularly in the area of initiating event-mitigating system interactions. The conclusions and insights it affords are usually reasonably sound if appropriate consideration is given to the uncertainties and if great numerical accuracy is not required for the particular application. Most important, system modelling has provided insights about the relationships among systems, failures and phenomena that could not have been obtained in any other way.

There continues to be rather large uncertainties in the *numerical* results of PSAs (core-melt frequency, off-site risk) for a variety of reasons. One key reason is that for some accident sequence initiators, the likelihood of the initiator is so low that such events have rarely, if ever, happened. In such cases (examples of which include very large pipe breaks, and especially Reactor Pressure Vessel failure, large earthquakes, and failures of the reactor protection system function), the PSA analysis must rely on synthesized estimates that are difficult to perform and uncertain because of the lack of data associated with them. For other initiators (including the more common transients, the smaller earthquake and minor fires) there is a valid data base that can be relied on in the analysis, and the uncertainties are smaller. It turns out that the numerical results of PSA are more reliable when the accident sequence quantification relies on combining several reasonably well-known rates and failure likelihood. On the other hand, the results are somewhat less reliable when the key numerical inputs are synthesized from various analyses and extrapolations rather than taken from direct observed experience.

4.3 Containment Analysis and Accident Sequence Development

This area includes analyses of the thermal hydraulic response of the plant to an accident, the progression of severe accidents and containment performance under severe accident loadings for accident sequences or groups of sequences. The analyses include a wide range of phenomena, some of which are not well understood.

In general, the validity of the analyses in these areas is not as good as in the plant system analysis. This is due largely to the lack of experimental results against which to compare the models. Some of the areas, especially radionuclide behaviour in post-melt environments, are sufficiently complex that it would be very difficult to construct models based on first principles even if results from realistic core-melt experiments were available. Whilst the entire area remains in a state of flux resulting from the widely perceived need for improvements and the results of current research, there are some trends developing towards exploitation and implementation of work already completed and these are reported further in Section 5.

Different models are required to model different phases in the progression of an accident: core degradation and melting within the vessel, steam and water circulation before vessel failure, the dispersal of the molten portion of the core upon vessel failure, core concrete interactions and the coolability of the debris bed on the containment floor. Structural analysis is needed to determine the response of the containment to thermal and pressure stresses. Hydrogen generation and mixing in the containment are of special concern. It is also necessary to estimate the amount of energy that can be released in steam explosions after the fall of the molten core into water in the bottom of the vessel or in the reactor cavity. Furthermore, specialized and detailed understanding of quite different aspects of phenomena may be required in applying PSA to different types of reactors. For example, such items as recriticality, Q^* (the energy released in a whole core accident) and sodium burning would need to be included for studies on LMFBRs, whilst other reactor types will have different special needs. Further, extending the coverage to nuclear chemical plant and criticality and to non-nuclear hazardous plant of all kinds needs specialist input at this point of the analysis to model particular accident sequence development. (See the papers accompanying this one for coverage of non-nuclear plant). It is not possible to generalize these brief remarks to cover the state of development of phenomena for all reactor types, nuclear plant or non-nuclear chemical plant. Specialist advice and input is needed.

4.4 Fission Product Transport

The characteriztics of radionuclide releases to the environment are described in terms of various timing and location parameters, the thermal energy release rate, and the quantities of radionuclides released, and also the quantities of radionuclides of the various elements available for release from the fuel and transported through the reactor coolant system, the containment, and possibly buildings external to the containment* before reaching the environment.

Analyses have shown that both natural and engineered retention mechanisms can significantly reduce the inventory of radionuclides available for release if enough time is available for those mechanisms to act. Therefore, source terms are strongly affected by whether or not the containment fails and, if it fails, by the time and the mode of failure.

Advances have also been made in the PSA analysis capabilities, including improved codes and methods for developing and quantifying containment event trees.

Shortly after the Three Mile Island accident, questions were raised about the appropriateness of the methods used to analyse source terms in the RSS and subsequent PSAs. In the face of complex problems and large gaps in the existing body of knowledge, the RSS chose to make conservative assumptions for source term predictions in some areas– for some of the radionuclides in certain accident sequences, the RSS methods estimate higher release fractions than we now believe would be observed in an actual accident. These over-predictions may be significant in many cases since the conservative assumption must be to assume 100% release. As a result of suspected deficiencies, a number of research programmes have been undertaken to improve the ability to

* The meaning here is to cover other transport pathways which might go via the service buildings or, in the case of Sizewell B, the tertiary containment.

model radionuclide release and transport in severe accidents realistically, and these are outlined in the next section.

Many uncertainties are associated with the predictions of severe accident progression, containment response and radionuclide transport. Few sensitivity studies were performed and the validation of models for the broad range of severe accident phenomena is extremely limited and *quantitative* uncertainty estimates are not generally available. As a minimum, current research can be expected to provide a better characterization of source term uncertainties and in some important areas reduce the conservatisms in PSA analysis.

4.5 Health, Environmental and Economical Consequence Analysis

The health and economic consequence analysis portion of a PSA provides estimates of the frequency distribution of possible off-site consequences for core-melt accidents. Models have been developed which describe the transport, dispersion and disposition of radioactive materials and predict their resulting interactions with the environment and the effect on the human population. Consequences can include early fatalities and injuries, latent cancer fatalities, genetic effects, land contamination and economic costs.

The validity in the area is relatively high, and the analysis methods have been quite stable for some years. One area where detailed improvements or specialist applications have been made is in the enhancement of models for the mitigation of radiation exposure (for example, evacuation and sheltering).

The first comprehensive assessment of consequences was performed in the RSS. Since that study, modelling capabilities have been improved, model and parameter evaluation studies have been performed and existing models have been applied to provide guidance in such areas as emergency planning and reactor siting. In addition, the importance of potential consequences resulting from releases of radioactive materials to liquid pathways has been examined.

Uncertainties in off-site consequence predictions have not yet been assessed comprehensively, although their magnitude can be inferred from the large body of existing parametric (or sensitivity) analysis in which consequences are calculated for a range of plausible values of a key parameter or model. The PSA ‘Procedure Guide’[50] made a tentative listing of the relative contribution to total uncertainty of the major parameters and models in an off-site consequence analysis. Important contributors to uncertainty were the magnitude of the source term, the form and effectiveness of emergency response, the rate of dry deposition (fallout during rainless periods) of particulate matter from the plume, the modelling of wet deposition (washout by rainfall) and the dose response relationships for somatic and genetic effects.

Ongoing research is focused on quantifying and, where possible, reducing uncertainties. Although uncertainties are likely to remain quite large, a thorough examination of their origin and magnitude will provide both a firmer basis for the application of consequence analyses and a better understanding of their limitations. A current major study (COSYMA) is being undertaken under the EU’s fourth Framework programme (in collaboration with the USA) to perform a comprehensive examination of uncertainties in consequence calculations. This is expected to make a significant contribution to this area.

4.6 External Events

External initiators are discussed separately, principally because the method for treating them is, in some respects, different from the method for treating so-called internal initiators. The external initiators differ from the internal initiators in that they are likely to cause important concurrent events that complicate the response of the plant to the initiator and may degrade off-site mitigation efforts. For example, a severe external flood is almost certain to affect the possible evacuation of the nearby population and an earthquake severe enough to damage the plant is also likely to cause a loss of off-site power and to disrupt evacuation plans seriously. External events include:

1. Earthquakes
2. Internally initiated fires
3. Floods (both external and internal)
4. High winds (tornadoes and hurricanes)
5. Aircraft, barge and ship collisions
6. Truck, train and pipeline accidents
7. External fires
8. Volcanoes
9. Turbine missiles
10. Lightning

For a specific site, it is necessary to identify which of these (and other hazards) must be considered. Not all apply to all sites!

The basic approach consists of quantifying the expected frequencies of the various initiating events, determining their effects on various pieces of equipment and determining the resulting effect of any degradation or failures on plant performance.

The validity of the analyses for many external initiators remains questionable because of the lack of appropriate experience against which to judge models or because the problems are inherently complex and difficult to treat. The methods of analysis for most of the external initiators are now reasonably mature; nevertheless the need for further improvement in the current treatment of most of the important initiators is recognized. These are discussed below.

The analysis of external initiators has seen major advances in the decade under consideration. However, the uncertainties associated with such analyses are still significantly larger than those associated with most internal initiating events, principally because of uncertainties associated with the development of the hazards curves (that is, the frequency of occurrence of an event exceeding a given magnitude). Nuclear power plants are carefully designed and engineered to be resistant to external initiators at the levels expected to occur. Taking normal design safety margins into account, the external initiators that are found to pose a significant threat to the plant are extremely severe and thus exceedingly rare. As might be expected, predicting the frequency of these unusual occurrences is very difficult and the resulting expected frequencies have very large uncertainties and the plant response tends to be of the 'cliff edge' variety leading to chaotic situations with multiple component and systems failures, as well as potential degradation of the key barriers to release of radioactivity.

For seismic events, a consensus prevails that the uncertainties in the core-melt frequency remain quite large for seismic PSA analyses. For these results, error factors of 10 to 30 (implying ranges of about 100 to 1000 for the 5 to 95% confidence interval) might be reasonable at present. A major contributor to this uncertainty is the likelihood of the very large earthquakes that dominate the analysis. These large numerical ranges for quantitative results do not negate the significant engineering insights obtained. Many of these insights are new and could not be acquired with traditional methods. In particular, the system vulnerabilities and common cause dependencies revealed have indicated areas where further investigation is warranted and where regulatory consideration may be required.

It is still too early to judge the achievable accuracy of the fire analysis methods. The uncertainties are probably larger than those for internal initiators, but the engineering insights obtained from the fire analyses performed to date have already been very useful and are in no way invalidated by the large uncertainties in the quantitative results. Methods developed for PSA are now finding application within the design basis in demonstrating the safety case for modern plant. PSA fire analyses have found major uses in analysis of Former Soviet Union (FSU) designed plant. In the years following Chernobyl and the generation of significant Western assistance, the identification of fire hazards and their rectification has been one of the most significant developments of these methods[53].

While engineering insights are available concerning vulnerabilities from high winds, the estimates of core-melt frequency or risk from them are highly uncertain due to the difficulties in determining the frequency with which wind speeds high enough to significantly damage a reactor may be expected.

Flooding analysis is complicated by several factors. The fragility of safety equipment (especially electrical equipment) exposed to the spray from an internal pipe or tank break is very difficult to analyse quantitatively. Flood-induced corrosion can compromise the ability of safety equipment to remain operable during the recovery period after a particular flood has been nominally 'controlled'. Another flaw in the analysis is the limited ability to quantify partial blockages of drains or sumps that are relied on to carry away flood waters. Finally, flooding (especially from an external source) can randomly deposit solid matter like sludge, silt or even sizeable objects in or on reactor plant equipment. These effects are difficult to analyse. The data base and analytical methods for coping with these issues are not well developed. Difficulties in modelling human intervention can also complicate the analysis.

External initiators such as aircraft impacts, pipeline accidents, external fires, volcanoes and turbine missiles are typically analysed probabilistically by performing a bounding analysis on their frequency of occurrence. An estimate is then made of whether the initiating event is serious enough to merit 'concern'. The main insight gained from the analyses performed on these 'other' initiators (numbers 5 through 10 in the list above) are that, generally, they have minor risk significance in the United States. However, for European situations, aircraft impact is seen as being of particular importance due to the large number of aircraft movements, particularly of military craft, in European airspace. In Germany this has led to special design provisions (the 'bunker' containment design). This indicates how PSA can be used as an important guide to an understanding of which issues must be taken seriously and which can legitimately be discounted at an early stage in the siting of hazardous plant. It also raises the issue of the relevance of the historical data bases since, post re-unification and the end of the Cold War, the type of military flights (mainly in the 1950s and 1960s of USAF Starfighters) which contributed to the statistical data base of aircraft crash rates in Germany have ceased.

4.7 Uncertainty Analysis

The preceding sections have discussed the sources of uncertainty in PSA results (parameter variation, modelling, completeness). Uncertainty analysis provides a framework for properly combining and describing the uncertainties associated with various elements of the analysis to determine the overall uncertainties associated with the results (for example, risk) or intermediate quantities (for example, sequence frequency). This is shown as 'linking' all the components of the PSA in Figure 13.

Risk analysts are only at the threshold of performing comprehensive uncertainty analyses. A variety of techniques have been used or proposed; however, many are still being developed and, in general, the methods have not been applied in all their combinations for all parts of the PSA. The uncertainties which are generally quantified in PSAs are those which are due to parameter or data uncertainties. Uncertainties which are due to alternative models or alternative assumptions need to be considered separately by sensitivity analyses. In specific cases, the effects of different modelling assumptions can be as large, or larger than, the uncertainties stemming from the data or parameter estimation.

Because of the different probability distributions which are used in PSAs to quantify parameter uncertainties, the propagated output probability distributions describing uncertainties in the results are themselves uncertain. Stated confidence or probabilities associated with given ranges (or error factors for the risk results) are consequently also uncertain. PSA uncertainties should be considered 'fuzzy' values that account principally for the input parameter uncertainties which have been explicitly quantified.

The significance of many of the modelling simplifications and assumptions which exist in a PSA can be revealed by performing sensitivity studies to evaluate the impacts of model alternatives and different assumptions. They can also be treated by assigning uncertainties to parameters subjectively and propagating these uncertainties.

Well-developed methods are available for estimating uncertainties in the parameters derived from the basic data and propagating them through the analysis. While the two principle approaches used differ, they may produce similar results, particularly when the data base is large. They can also differ substantially, reflecting the assumptions on which they are based.

Uncertainty and sensitivity analyses need to be better

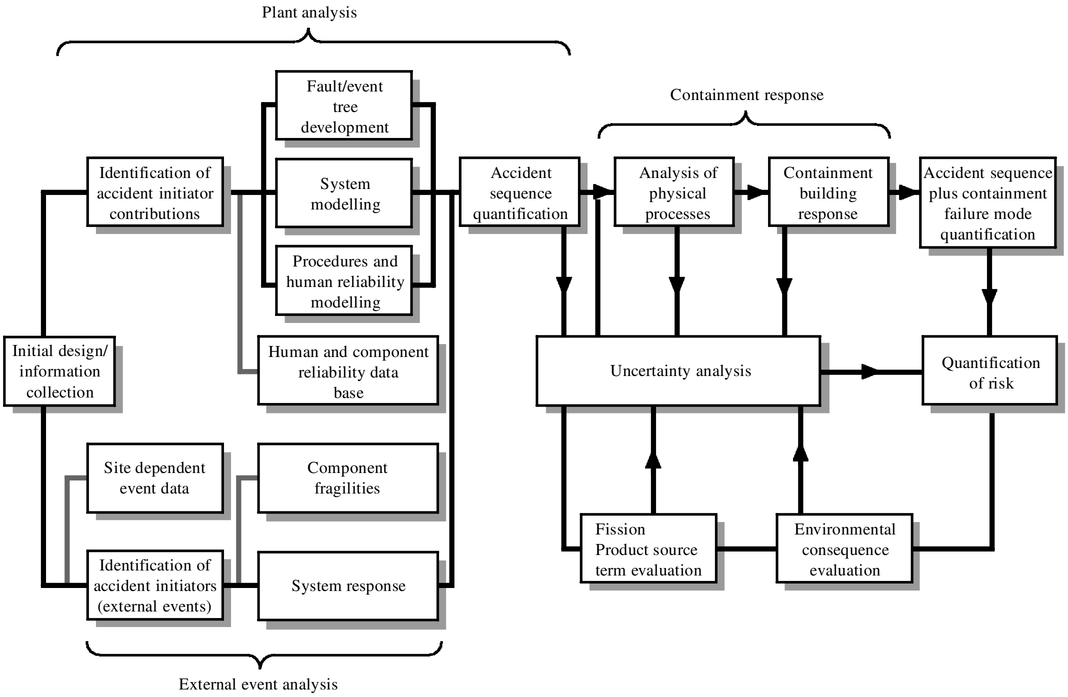
Plant analysis
Fault/event tree development
Containment response
Identification of accident initiator contributions
System modelling
Accident sequence quantification
Analysis of physical processes
Containment building response
Accident sequence plus containment failure mode quantification
Procedures and human reliability modelling
Initial design/ information collection
Human and component reliability data base
Uncertainty analysis
Quantification of risk
Site dependent event data
Component fragilities
Fission Product source term evaluation
Environmental consequence evaluation
Identification of accident initiators (external events)
System response
External event analysis

Figure 13. 'Linking Diagram' showing the connection between the various steps in a PSA and in particular showing the central role of the uncertainty analysis.

organized and displayed. The sensitivity and uncertainty analyses that are performed in a PSA have not always been well organized and discussed together in one place in the report. If this is done, it will provide a better understanding of the dominant uncertainty contributors, aid in identifying robust uses of the results and better identify areas where additional research is needed.

4.8 Summary of the State of the Art of PSA

The following represents a minimal summary of the state of the art of PSA following its rapid development from ~ 1975–1985.

System modelling (plant analysis)
- Methodology basically unchanged since RSS.
- Improved computer codes now allow efficient handling of more complex models.
- Improved treatment of dependent failures.

Human interactions
- Improved techniques for handling procedural errors.
- Cognition and comprehension errors are often considered but modelling is still relatively crude.
- Analysis now includes recovery actions, but further improvement is needed.

Data base
- Significant improvement for transient initiators.
- Only modest improvement in other areas.
- Accident progression, containment response and radionuclide transport.
- Significant improvement in analytical abilities.
- Area currently undergoing rapid change.
- Generally only subjective uncertainty estimates currently available.
- Limited experiments to provide validity in some areas.

Consequence analysis
- Some improvement in modelling capabilities.
- Sensitivity analyses available for many modelling assumptions.
- Comprehensive uncertainty analysis not yet available.

External initiators
- Major advances in recent years.
- Great confidence cannot be placed in quantitative results of low frequency events.

Uncertainty analyses
- Some improvements in methods.
- Comprehensive treatment not yet available.

5. SEVERE ACCIDENT RESEARCH AND DEVELOPMENT

One of the most important ramifications of the development of PSA has been its voracious need for information. The quantitative approach to risk evaluation means that there is 'nowhere to hide' when it comes to the need for information and understanding. When the RSS was performed, its main contribution was to expose areas of lack of knowledge or data, or where 'engineering judgement' had been used in situations where judgement was hardly appropriate. The need for more information was brought into sharp focus by the TMI-2 accident and the regulatory responses to it. This spawned an intensive R&D programme, generally labelled 'Severe Accident' research, which began in earnest around 1980 and in some areas continues to this day. Any history of the development of the PSA methodology would be incomplete without some reference to the major R&D it engendered, and the tangible improvements in safety which have ensued.

Whilst methods have been refined, and data bases improved, the developments in reliability analysis have not required an extensive research programme. The topic area is rather mature and hence the value of level 1 PSA (which described component and systems features up to core degradation) has been recognized and its output is now virtually commonplace for a variety of uses. For level 2 PSA in particular the implementation of the methodology served rather to highlight the paucity of models and data needed to follow the evolution of a degrading core both in- and ex-vessel, and in the requirement to understand containment response sufficiently well to be able to predict radioactive source terms to be expected with specific accident sequences. Apart from human factors (which I return to shortly), it has been with the phenomenology of core degradation that much of the R&D has been focused.

All countries operating reactors for power generation have actively participated in this programme, and the level of international collaboration has been almost uniquely high. The international institutions (the IAEA, Organization for Economic and Cultural Development (OECD)/Nuclear Energy Agency (NEA), World Association of Nuclear Operators (WANO), etc.) have also played very active roles. This has meant that research results in the majority of the areas have been made freely available to all countries, as have been the consequent safety benefits. There are two main reasons for this. First, there is a common interest in research which leads directly to an improvement in safety, and second, many of the research areas are technically complex and must operate with difficult materials in extreme conditions. They are therefore very expensive. A good example of such collaborations is the European Union's Severe Accidents research programme which has been organized and paid for by the Nuclear Fission Safety Programme of the EURATOM Framework programme (Council decision 94/268/Euratom of 26 April 1994).

It is anticipated that a similar programme will continue under the fifth Framework programme beginning in 1999. The EU's programme in Severe Accident research has had a mid-term review[54]. A quotation from the foreword of this review by E. Andretta, the Director of the relevant section of the Commission, sums up the 'international' view of such research:

'The subject of hypothetical severe accidents in LWRs is so complex to understand, the relevant research is so expensive, that international research programmes, such as the present one, are needed to come to firm conclusions. Through these EU research projects, the outline spectrum of severe accident problems is being addressed, from early accident progression in the primary coherent system, threats to the reactor pressure vessel and radiological releases out of the primary circuit, up to severe damage to containment integrity, assuming that the safety systems are not working satisfactorily. Technological solutions are also investigated, especially for mitigative measures against the consequences of severe accidents. In addition, some R&D efforts are being devoted to risk relevant aspects of materials ageing.'

Virtually all of the topics mentioned here have been spawned out of the need to have an improved understanding of the basic mechanisms of the core melting behaviour, and workable models so that level 2 PSA can be refined into a viable tool. Similar research programmes have been actively funded in the USA (mainly through the USNRC[55]) and in all LWR operating countries. In the UK this is co-ordinated by the Nuclear Safety Directorate of the Health and Safety Executive, and managed by a joint industry/NII group.

Whilst there are still a number of open issues, much of this research is now mature and the resources available both nationally and internationally have been reducing in recent years. This generally follows the trend in other aspects of the nuclear industry where the building programme is moribund and the attention has refocused somewhat onto issues relating to plant ageing (which also have their severe accident elements) and into radionuclide waste management. This has caused concern in many research circles since expensive core specialized facilities and capabilities are in jeopardy and because there is always more knowledge to be unearthed,. In recognition of that, the Committee on the Safety of Nuclear Installations (CSNI) of the OECD/NEA has initiated a study of this possibility to co-ordinate specific international collaborations where such facilities are deemed to have real safety significance for many countries. This work has been reported in a series of documents[56], the latest of which is in the final stages of preparation.

Current applications are focusing on what can be done to mitigate and/or manage severe accidents, and a full review of developments is available[57]. In addition, a recent review of the technical issues underpinning the remaining uncertainties in severe accident phenomenology is also available[58].

6. THE REGULATORS' VIEWS OF PROBABILISTIC METHODS

The early developers of PSA believed that the capability to 'calculate' risks posed by plant (and this applied to all potentially hazardous plant as exemplified by the papers accompanying this one) would find use not only with plant operators and designers but also with regulators. After all, the *acceptability* of a plant in the broadest sense has to be a combination of risks (health, environmental and economic) and benefits[59]. The ability to have a firm quantification of the actual risk posed to people is an essential contribution to this process[60]. This review began with the early (1967) attempts by Farmer to provide a criterion against which risks may be judged– it led eventually to the development of the methods of PSA in order to calculate the risk so that compliance with a criterion could be judged. This process itself led to a much deeper understanding of risk and the problems connected with calculating it and, in time, led the regulatory authorities to regard PSA with some caution. In the UK, much of this debate took place at the Public Enquiry called over the then CEGB's application to build a PWR at Sizewell in Suffolk (The Sizewell B Inquiry). This debate focused on *risk acceptance* and risk quantification with much discussion surrounding the nature and importance of uncertainties in what is already a probabilistic case. The whole question of risk *acceptance* criteria was discussed with the Inspector himself almost complaining that the industry (CEGB) had set out to *calculate* risk, but the regulator (NII) had failed to provide any guidance as to what might be deemed to be an acceptable level. Indeed, he charged the NII with undertaking a wide-ranging debate on this topic and in formulating its authoritative advice. This was done in 1988 with the publication of the so-called 'Tolerability of risk' paper[61]. For a full analysis of the many aspects of risk acceptance see Reference 6, for example. The Public Inquiry was an extremely valuable forum in which to discuss risk. The lawyers on both sides and the Inspector and his assessors were all very keen to understand and interpret these data and, after all, represented some of the best legal brains in the land. It is doubtful if full benefit has yet been gained from those deliberations and the Inquiry itself as to the optimal use of PSA in a non-technical forum. The comments of the Inspector (Sir Frank Layfield)[62] illustrate the point.

Thus in paragraph 2.26:

'Probabilistic risk information can offer the public a useful measure of the potential risk from the plant. But the technique is at an early stage. Effort needs to be put into improving the presentation of the results so that their use and limitations can be properly understood. I believe that if it is successfully done, the use of probabilistic risk estimation could and should become increasingly widespread within the nuclear industry and elsewhere.'

And again in paragraph 2.51:

'I conclude that (a) the most meticulous and exhaustive attention must be paid to minimizing the occurrence and effects of human errors. The risks from human error might otherwise exceed other risks from Sizewell B.'

This is not the place to discuss whether these statements are technically correct, but to note that even the Inspector felt the need to have risks and uncertainties presented in a more transparent fashion.

A number of papers have been published[63] by various players in the Sizewell Inquiry which expand on *their* view of its utility, and on problems associated with it.

Underpinning all of the questions surrounding PSA and its use as a licensing tool is the question of uncertainty. With PSA the analyst and assessor have nowhere to hide. As I said in the introduction, it makes *explicit* the demands for data and models, where they may well not exist. The RSS pointed this out very early on. Even though uncertainties exist, and will no doubt continue to exist in some areas, plant still need to be licensed. However, *all* regulatory bodies have shied away from treating uncertainties in the bald 'up front' way presented via a probabilistic calculation. For example, consider the NII's views as expressed by its witness at the Sizewell B Inquiry.

Sizewell B Inquiry daily transcripts day 165, page 89 E-F and in a written response NII/P/2 (Addendum 14). In the latter reference (paragraph 10.1) we have:

'The Inspectorate takes the view that PSA is an important technique in producing a safe balanced design and in providing a unifying framework for assisting the safety case. It does, however, have significant limitations as described above [not reproduced here]. The Inspectorate does not consider that the effort required to produce a formal confidence calculation, for example, as described in Section 4(ii) of CEGB P/16 Addendum 4[64], would be warranted in view of those features to which it could not sensibly be applied. Accordingly, it does not require such calculations to be performed as a condition for licensing Sizewell B, nor does it anticipate imposing such requirements in the future, although it will review the situation as work in this area develops.'

(The comment in square brackets is the author's addition.)

It is important to note that some 15 years on that this is still the case.

In the UK, therefore, PSA has not become the once-hoped-for all-encompassing tool for regulation which would take the evaluation of the acceptability (or more properly the tolerability) of risk as a major plank in the regulatory process. This is discussed more fully in Reference 65.

This situation also pertains in all OECD countries. In the USA, where PSA has been developed to a very high degree, the NRC advocates the use of risk *informed* regulation, but stops short of specific risk-based regulatory criteria, even in its latest guidelines (10 CFR53)[66] for advanced plant. However, the NRC has produced a guidance document for its staff on the uses of PSA[67] and very recently (February 1999), the ASME brought out a 'standard' for PSA which was just going out for public comment as this review was being completed.

In conclusion, PSA has not lived up to its early promise as a licensing tool. However, it is widely seen as a key methodology and one which has become an adjunct to, if not a front-line part of, nuclear regulatory practice.

7. SUMMARY AND MESSAGES FOR THE FUTURE

There is no doubt that the period from 1975 (publication of the RSS) to 1990 (publication of NUREG 1150[68]) saw an explosive increase in the number of full PSAs. Table 5 lists a representative sample of these (without giving detailed individual references). At the end of this period, a very large amount of knowledge had been gained on a wide range of technical issues concerned with the 'nuts and bolts' of implementing the methodology. Amongst these were elaborate schemes for propagating uncertainties, so-called 'delphic' techniques used to give some discipline and transparency to the use of expert judgement* (see Reference 69), advanced suites of computer codes for accident sequence analysis and major improvements and sophistication in containment and containment function analysis. Describing the phenomenology associated with accident progression is so complex that it is now normal to use combinations of large codes, each developed and validated using 'separate effects' experiments and modelling. Examples of this include the French ESCADRE and ICARE codes[70] and the ESTER fission product transport code suite developed for the European Union at the ISPRA Laboratory[71].

The methodology was (and still is!) expensive; a 'full'

* Note that expert judgement still plays a role at the end of this period (and indeed it still does). This is an apparent contradiction to what is meant by a fully quantitative methodology. The point here is that the use of judgement must be transparent and testable; that is the real advance over the methods of the RSS.

level 3 PSA, with an external events analysis, would require more than 100 man years of skilled effort and may cost many tens of millions of dollars. Nevertheless, it had by then evolved into an effective and comprehensive package of methodologies with great potential for use on all kind of complex plant.

It is perhaps fitting that the end of this development period is marked by another major work from the USNRC, this being NUREG 1150[22]. This took full PSAs performed on five plants in the USA (Surrey Unit 1, Peach Bottom Unit 2, Sequoyah Unit 1, Grand Gulf Unit 1 and Zion Unit 1) with the basic objective of providing a comprehensive statement as to the state of the art and, perhaps because of the sensitivity of the issues and the very real technical challenges, was extensively reviewed. For the draft report these reviews were performed by:

- Kouts Committee;
- Kastenbeg Committee;
- American Nuclear Society;
- Advisory Committee on Reactor Safety;

and for the second draft:

- Special Committee to Review the Severe Accident Risk report (an international committee formed under the provisions of the Federal Advisory Committee Act);
- American Nuclear Society Special Committee on NUREG–1150 and Advisory Committee Reactor Safeguards.

The membership and comments of these committees are given in Volume 3 of NUREG 1150[22].

From that point on, the development of PSA becomes fragmented, with specialists involvement in many aspects. The methods are widely used, but rarely all together and hardly at all at level 2 or level 3– a full calculation of the risk spectrum is not usually attempted. There are some obvious reasons for this.

- No *new* plants are being built, so PSAs are not called for either at the design stage or for regulatory or operational purposes.
- The development of advanced (next generation) plant has focused on a few designs (the European Power Reactor (EPR), the Westinghouse AP600 and the ABB Combustion Engineering Systems80+) and these have all had probabilistic methods applied at the design stage.
- There is little or no regulatory pressure to pursue PSA beyond that presently considered prudent, and that means *not* to form a licensing requirement, or the basis for comparison against probabilistic safety goals. However, note that one of the key guiding principles for the design of the EPR[45] is that no accident (including severe accidents with core melting) should require off-site emergency measures. This is derived from PSA results and the design of the plant and the judgement as to whether it has met this requirement will have to be made on probabilistic arguments.
- The principal current concern is with the materials and ageing issues of the existing stock of nuclear power stations, at least in the West. Here, the challenge is to continuously update the relevant data bases and systems performance calculations so that there is a realistic appraisal of current and future risks, and not just to the risk which may have been calculated at the beginning of life.

In fact, the most active use of PSA in recent years seems to have been in attempts to demonstrate the safety (or otherwise) of the RBMK and VVER reactors in the FSU and Eastern Europe. These have to be treated with caution as the provenance of some of the data used is questionable, but generally speaking the calculations performed in 'Eastern Europe' (Hungary, Czech and Slovak Republics or Slovakia) are of good quality. A rather special case is the so-called 'Barselina' PSA (a combination of Barsebaeck in Sweden and Ignalina (the RBMK in Lithuanian)) which was a joint Swedish-Lithuanian project carried out with the specific aim of improving the safety of this particular plant and especially to produce Emergency Operating Instructions (EOIs).

To give some indication of the range of applications of PSA, or at least component parts of it, which are being followed up actively at present, the following list is presented for illustration:

- Living PSA– PSA schemes which have been simplified and used to upgrade the risk profile of the plant continuously. Normally restricted to level 1, and using core-melt frequency as the benchmark. These are focused on specific plant, or even sub-systems of plant, so that the generic reliability data base which is the starting point for the initial PSA is slowly replaced by data obtained on the components and systems and maintenance history of the plant in question.
- Shutdown PSA– Studies aimed at the special conditions existing when a reactor is shut down for its refuelling stage. There are indications that this can be a very significant contribution to risk.
- Seismic PSA– Analysis focusing entirely on the plant's response to earthquakes, usually in areas of relatively high seismicity, to identify particular dependent facilities.
- Fire PSA– A subset of PSA now commonly performed on older plant (especially in the FSU) as this provides arguably the most risk reduction per unit of analytical effort.
- Risk-informed maintenance– Using level 1 PSA to optimize maintenance, both at shutdown and whilst the plant is on line[72].
- Probabilistic Fracture Mechanics– This subset of PSA is used to evaluate the materials properties of structural steels, especially the embrittlement of steel and welds under irradiation. It has evolved into a significant technical discipline in its own right. The principal focus of development was the analysis of the reactor pressure vessel reliability for the Sizewell B reactor and is discussed in the 'Marshall Report'[73].

These represent a sample of the activities being carried forward under a banner of Probabilistic Methods.

For the future, I believe that the immediate focus will be on the improvement in accessibility and transparency of probabilistic methods for a whole range of 'operational' applications (risk-informed maintenance, design, optimization of Station and Emergency Operating Instructions, etc.). Some of the major sources of concern will continue to be tackled, primarily the inclusion of refined quantifiable human factors models, the treatment of uncertainties and dependent failures and some serious attempts to ensure that the reliability of digital (software) based systems is improved. However, it remains the fact that the next phase of *real* development of PSA awaits a rekindling of reactor ordering and a buoyant nuclear market.

REFERENCES

1. *IAEA Report of the Advisory Group on Development of a Manual for Probabilistic Risk Analysis and its Application to Safety Decision Making, 14–18 May 1984* (IAEA, Vienna).
2. *Shorter Oxford Dictionary on Entomological Principles*, 3rd edition, 1970, p. 1743.
3. Royal Society, 1983, *Risk Assessment: A Study Group Report, and 1992, Risk: Analysis, Perception and Management: Report of a Royal Society Study Group* (Royal Society).
4. Jones, D. A. (ed), 1992, *Nomenclature for Hazard and Risk Assessment in the Process Industries*, 2nd edition (Institution of Chemical Engineers).
5. British Medical Association, 1987, *Living with Risk* (John Wiley and Sons).
6. Allen, F. R., Garllick, A. R., Hayns, M. R. and Taig, A. R., 1992, *The Management of Risks to Society from Potential Accidents* (Elsevier Applied Science).
7. See Reference 6, Chapter 5.
8. Le Guen, J., 1995, *Generic Terms and Concepts in the Assessment and Regulation of Industrial Risks*, Health and Safety Executive discussion document.
9. Covello, V. T. and Munpower, J., 1985, Risk analysis and risk management: an historical perspective, *J Risk Analysis*, 5 (2): 103–120.
10. Bernstein, D. L., 1997, *Against the Gods* (John Wiley and Sons).
11. Ashby, E., 1978, *Reconciling Man with the Environment* (Oxford University Press).
12. Green and Bourne, 1972, *Reliability Technology* (Wiley) (reprinted 1982).
13. Kececioglu, D., 1993, *Reliability and Life Testing Handbook* (Prentice Hall).
14. Hayns, M. R., The implications of PRA for safety policy, in Cullingford, M. C., Shah, S. M. and Gittus, J. H. (eds), 1987, *Implications of Probabilistic Safety Assessment*, 27–41 (Elsevier Applied Science).
15. Kinchin, G. H., Risk assessment, in Marshall, W. (ed), 1983, *Nuclear Power Technology*, Volume 3 (Clarendon Press, Oxford).
16. Siddall, E., 1959, Statistical analysis of reactor safety standards, *Nucleonic*, 17 (2): 64.
17. Howard, R. W., Barthrop, R. K., Bishop, G. S. and Bevan, F., Reliability in automatic landing, *Flight*, 10 October 1960.
18. For a complete and authoritative account of the Windscale accident and the history of the development of nuclear power around this time, see Gowing, M., 1987, *How Nuclear Power Began* (University of Southampton Press).
19. Marley, W. G. and Fry, T. M., 1956, Radiological hazards from an escape of fission products and the implications for nuclear power reactor location, *Proc Int Conf on the Peaceful Uses of Atomic Energy*, 13: 102–105 (United Nations, New York).
20. Farmer, R., 1967, Siting criteria– a new approach, *Containment and Siting of Nuclear Power Plants Proceedings of a Symposium, IAEA SM 89/34* (IAEA, Vienna).
21. *Reactor Safety Study, An Assessment of Accident Risk in US Commercial Nuclear Power Plants*, USNRC WASH 1400 (NUREG 75/014), October 1975.
22. *Severe Accident Risks: An Assessment for Five US Nuclear Power Plants*, USNRC NUREG 1150, December 1990.
23. See for example Battelle Memorial Institute (BMI) Report 2104, July 1984, *Radionuclide Release under Specific LWR Accident Conditions*, and Gittus, J. H. (ed), 1983, *PWR Degraded Core Analysis*, UKAEA Report NDR (610).
24. Westinghouse Electric Corporation, *Sizewell B Probabilistic Safety Study*, WCAP 9991, July 1992.
25. Ottway, H. J. and Endman, R. P., 1970, Reactor siting from a risk point of view, *Nuclear Engineering and Design*, 13: 305–376.
26. In principle both RPV failure and interfacing systems LOCA should be viewed as 'simple' systems failures but the ways in which they are dealt with are anything but simple. In the UK the ramifications of this were exemplified in the Sizewell B study and the NII's stated approach to large accidents– these are discussed in Section 6.
27. *The Three Mile Island Reactor Pressure Vessel Investigation Project– Achievements and Significant Results*, OECD/NEA and USNRC Open Forum, OECD, Paris 1994.
28. See for example papers in *Severe Accident Management Implementation*, OECD Specialists Meeting, Niantic, CT, USA, 12–14 June 1995.
29. US Nuclear Regulatory Commission, February 1981, *A Risk Comparison*, NUREG/CR 1916, and the discussion in Reference 8.
30. Commonwealth Edison Co., 1981, *Zion Probabilistic Safety Study.*
31. Consolidated Edison Co. and New York State Power Authority, 1980, *Indian Point Probabilistic Safety Study.*
32. US Nuclear Regulatory Commission, February 1982, *Safety Goals for Nuclear Power Plant, A Discussion Paper*, NUREG 0880.
33. US Nuclear Regulatory Commission, June 1980, *Report of the Task Force on Interim Operation of Indian Point*, NUREG 0715.
34. Testimony before the Nuclear Regulatory Commission, September 1984 (Testimony of F. Rowsome, USNRC).
35. Brearly, I. R., Nixon, W. and Hayns, M. R., 1987, An investigation of the closure problem applied to reactor accident source terms, *Implications for Probabilistic Risk Assessment*, IAEA SR 111/37 (Elsevier Applied Science).
36. See for example *Fire and Safety '94, 5–7 December 1994, Barcelona* (Nuclear Engineering International). In particular, Hayns, M. R., Fires and external hazards in Soviet designed plant– insights from Western assistance programmes (pp. 349–352) and Marttila, J., Fire risks in Soviet designed NPPs (pp. 353–365).
37. Sizewell B Power Station Public Inquiry, Mathews, R. R., The CEGB Safety Policy, CEGB Proof P/2 to the Sizewell B Public Inquiry.
38. Sizewell B Power Station Public Inquiry, CEGB Statement of Case, CEGB 1 Vol. 2, 139–143.
39. Sizewell B Power Station Public Inquiry, Wood, P. B., Proof of Evidence of HM Nuclear Installations Inspectorate's view on the CEGB's safety case, NII/P/2.
40. Richardson, D. C. *et al.*, A decade of experience of PRA in the USA– what has been achieved?, *IAEA Symposium on Safety Codes and Guides (NUSS) in the Light of Current Safety Issues, Vienna, 29 October–2 November 1984*, IAEA - SM-275/38.
41. Westinghouse Electric Corporation Sizewell B Probabilistic Safety Study, WCAP 9991, July 1982.
42. Sizewell B Power Station Public Inquiry, Gittus, J. H. *et al.*, CEGB Proof of Evidence, P/16, Addendum 3.
43. *The EPR Project, European Nuclear Society Conference Report*, Strasbourg, 13–14 November 1995.
44. Pederson, T., 1989, PIUS: status and prospects, *IAEA Bulletin 3*, 25–29.
45. Shepherd, J. and Hayns, M. R., 1991, SIR: reducing size can reduce costs, *Nuclear Energy*, 30 (2): 85–93.
46. *MW (Th.) MARS Nuclear Power Plant, Design Progress Report*, 1997 (University of Rome 'La Sapienza').
47. See for example Hayns, M. R. and Hicken, E. F., Key issues for passive safety, *IAEA Advisory Group Meeting on Technical Feasibility and Reliability of Passive Safety Systems, 21–24 November 1987, Julich, Germany*. And Hayns, M. R. and Phillips, D. W., 1987, Safety principles for advanced plant, *Nuclear Power Performance and Safety. IAEA International Conference, 28 September–2 October 1987, Vienna, Austria*, IAEA-CN-48/210, 459–471.
48. Deutsche Riskostudie, Kernkraft Werke, Verlag, TUV, Rheinland, 1980. See also Birkhoffer, A., 1980, The German risk study for nuclear power plants, *IAEA Bulletin*, 22 (5/6): 23–33.
49. *A Probabilistic Safety Assessment of the Standard French 900MW9e Pressurised Water Reactor*, CEA, IPSN, EPS 900, April 1990.
50. US Nuclear Regulatory Commission, September 1984, *Probabilistic Risk Assessment Reference Document*, NUREG 1050.
51. Hayns, M. R., Abbey, F., Clough, P. N. and Dunbar, I. H. (UKAEA) and Walker, D. H. (Westinghouse), November 1982, *The Technical Basis of 'Spectral Source Terms' for Assessing the Uncertainties in Fission Product Release during accidents in PWRs with special reference to Sizewell B*, UKAEA Report SRD R256.
52. See for example Norros, L., 1998, Evaluation and development of process operators' working practices, *Symposium of the Finnish Research Programme on Reactor Safety. VTT Automation*, 187–198, and references contained therein.
53. See papers in *Fire and Safety '94, 5–7 December 1994, Barcelona, Spain* (Nuclear Engineering International Ltd and Status Meetings Ltd).
54. Van Goethem, G., Kleinhurst, G., Marten Bernejo, J. and Zurita, A. (eds), 1997, *FISA– 97 EU Research on Severe Accidents, EC, Luxembourg 17–19 November 1997*, EUR 18258 EN.
55. See for example Spies, T. P., Lee, R. Y., Solfer, L. and Meyer, R. O., 1992, LWR severe accident source term research in the USA, in Kriscler, W. and Rubenstein, M.C. (eds), *The Phebus Project* (Elsevier Applied Science).

56. OECD/NEA, 1997*, Nuclear Safety Research in OECD Countries– Capabilities and Facilities.*
57. Livelent, M., 1997, Severe accident management for existing reactors– perspectives for future reactors, *FISA– 97 EU Research on Severe Accidents*, EUR 18258 EN, 15–28.
58. Henry, R. E., 1995, Overview: uncertainties remaining in severe accident phenomenology, *OECD International Conference on Severe Accident Management Implementation, Niantic, CT, USA, 12–14 June 1995*, paper No. 29.
59. See for example Chicken, J. E. and Hayns, M. R., 1989, *The Risk Ranking Technique in Decision Making* (Pergamon Press).
60. Hayns, M. R., 1988, Consequence assessment in nuclear power plant safety, *Radiation Protection in Nuclear Energy, IAEA International Conference, Sydney, Australia, 18–22 April 1988*, IAEA CN 51/88, 449–465.
61. Health and Safety Executive, 1998, *The Tolerability of Risk from Nuclear Power Stations* (HMSO, London).
62. Sir Frank Layfield, *Sizewell B Public Inquiry Report* (HMSO, London).
63. Cullingford, M. C. and Shah, S. M. (eds), 1987, *Implications of Probabilistic Risk Assessment* (Elsevier Applied Science), particularly Jenkins, P. D., The use of probabilistic safety assessment methods for CEGB reactors (pp 523–539), Campbell, J. F., The role of probabilistic safety assessment and the licensing of Sizewell B (pp 611–626), and Siddall, E., The logic of risk assessment (pp 739–753).
64. Sizewell B Power Station Public Enquiry, CEGB Proof of Evidence CEGB P/16 Addendum 4.
65. Roberts, L. E. J. and Hayns, M. R., 1989, Limitations on the usefulness of risk assessment, *Risk Analysis*, 9 (4): 483–494.
66. USNRC Regulatory Guide (10 CFR53), 1994.
67. US Nuclear Regulatory Commission, 1994, *A Review of NRC Staff Uses of Probabilistic Risk Assessment*, NUREG 1489.
68. See Reference 23 and the following supporting documents:
    1. Accident frequency analysis: NUREG CR 4550.
    2. Accident progression: NUREG CR 4551.
    3. External events methods: Bohn, M. P. and Lambright, J. A., November 1990, *Procedures for the External Event Core Damage Frequency Analysis for NUREG 1150*, NUREG CR 4840, SAND88-3102 (Sandia National Laboratories).
    4. Source term analysis: Denning, R.S. *et al.*, July 1986, *Report on Radionuclide Release Calculations for Selected Severe Accident Scenarios*, NUREG CR 4624, Volumes 1–5, BMI 2139 (Battelle Columbus Division). And NUREG CR 5263, Volume 6, BMI 2139, August 1990.
    5. Accident management analysis: Camp, A. L. *et al.*, September 1988, *The Risk Management Implications of NUREG 1150 Methods and Results*, NUREG CR 5263, SAND88 3100 (Sandia National Laboratories).
    6. QA studies: Cybulskis, P., November 1989,*Assessment of the XSOR Codes*, NUREG CR 5346, BMI 2171, (Battelle Columbus Division). And Dobbe, C. A. *et al.*, February 1990, *Quality Assurance and Verification of the MACCS Code Version 1.5*, NUREG CR 6376, EGG 2566 (Idaho National Engineering Laboratory).
    7. Code descriptions: Iman, R. L. and Shortencarrier, M. J., August 1986, *A User's Guide for the Top Events Matrix Analysis Code (TEMAC)*, NUREG CR 4598; SAND86 0960 (Sandia National Laboratories). And Iman, R. L. and Shortencarrier, M. J., June 1984, *A Fortran 77 Programme and User's Guide for the Generation of Latin Hypercube and Random Samples for Use with Computer Models*, NUREG CR 3624, SAND83 2365 (Sandia National Laboratories).
69. Pyy, P. and Pulkkinen, U., 1998, Risk and reliability analysis (LURI) and expert judgement techniques, *The Finnish Research Programme on Reactor Safety, VTT Symposium 189*, 163–177.
70. Rocreax, M. and Gauvain, J., 1997, ESCADRE and ICARE code system, in Van Goethem, G., Kleinhurst, G., Marten Bernejo, J. and Zurita, A. (eds), *FISA– 97 EU Research on Severe Accidents, EC, Luxembourg 17–19 November 1997*, EUR 18258 EN.
71. Jones, A. V. and Sheperd, I., ESTER– a European source term evaluation system, in Van Goethem, G., Kleinhurst, G., Marten Bernejo, J. and Zurita, A. (eds), *FISA– 97 EU Research on Severe Accidents, EC, Luxembourg 17–19 November 1997*, EUR 18258 EN.
72. See for example, Knoll, A., 1996, Quantitative risk matrices for on-line maintenance at a nuclear power plant, *ANS Annual Meeting, Reno, Nevada, June 1996*, 260–261 (PSE&G, Hancocks Hill).
73. Study group under the chairmanship of Lord Marshall, 1983, *An Assessment of the Integrity of a PWR Pressure Vessel* (UKAEA).

ADDRESS

Correspondence concerning this paper should be addressed to Professor M. R. Hayns, School of Engineering and Applied Science, Aston University, Aston Triangle, Birmingham B4 7ET, UK.

The manuscript was received 18 January 1999 and accepted for publication after revision 12 March 1999.