CSNI REPORT 124
RESTRICTED

OECD

NEA

A SURVEY OF THE APPLICATIONS MADE OF THE RESULTS OF PROBABILISTIC SAFETY ANALYSES OF NUCLEAR POWER PLANTS

Final Report of Task 2 of CSNI Principal Working Group No.5

OCTOBER 1986

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS
OECD NUCLEAR ENERGY AGENCY
38, boulevard Suchet, 75016 Paris, France

PRINCIPAL WORKING GROUP NO. 5 ON RISK ASSESSMENT

Task 2

Survey of Applications Made of the Results of
Probabilistic Safety Analyses of Nuclear Power Plants

NEA

The OECD Nuclear Energy Agency (NEA) was established on 20th April 1972, replacing OECD's European Nuclear Energy Agency (ENEA, established on 20th December 1957) on the adhesion of Japan as a full member.

NEA now groups all European Member countries of OECD and Australia, Canada, Japan and the United States. The Commission of the European Communities takes part in the work of the Agency.

The primary objectives of NEA are to promote co-operation between its Member governments on the safety and regulatory aspects of nuclear development, and on assessing the future role of nuclear energy as a contributor to economic progress.

This is achieved by:

- encouraging harmonization of governments' regulatory policies and practices in the nuclear field, with particular reference to the safety of nuclear installations, protection of man against ionizing radiation and preservation of the environment, radioactive waste management, and nuclear third party liability and insurance;

- keeping under review the technical and economic characteristics of nuclear power growth and of the nuclear fuel cycle, and assessing demand and supply for the different phases of the nuclear fuel cycle and the potential future contribution of nuclear power to overall energy demand;

- developing exchanges of scientific and technical information on nuclear energy, particularly through participation in common services;

- setting up international research and development programmes and undertakings jointly organised and operated by OECD countries.

In these and related tasks, NEA works in close collaboration with the International Atomic Energy Agency in Vienna, with which it has concluded a Co-operative Agreement, as well as with other international organisations in the nuclear field.

CSNI

The NEA Committee on the Safety of Nuclear Installations (CSNI) is an international committee made up of scientists and engineers who have responsibilities for nuclear safety research and nuclear licensing. The Committee was set up in 1973 to develop and co-ordinate the Nuclear Energy Agency's work in nuclear safety matters, replacing the former Committee on Reactor Safety Technology (CREST) with its more limited scope.

The Committee's purpose is to foster international co-operation in nuclear safety amongst the OECD Member countries. This is done in a number of ways. Full use is made of the traditional methods of co-operation, such as information exchanges, establishment of working groups, and organisation of conferences. Some of these arrangements are of immediate benefit to Member Countries, for example by improving the data base available to national regulatory authorities and to the scientific community at large. Other questions may be taken up by the Committee itself with the aim of achieving an international consensus wherever possible. The traditional approach to co-operation is reinforced by the creating of co-operative (international) research projects, such as PISC and LOFT, and by a novel form of collaboration known as the international standard problem exercise, for testing the performance of computer codes, test methods, etc. used in safety assessments. These exercises are now being conducted in most sectors of the nuclear safety programme.

The greater part of the CSNI co-operative programme is concerned with safety technology for water reactors. The principal areas covered are operating experience and the human factor, reactor system response during abnormal transients, various aspects of primary circuit integrity, the phenomenology of radioactive releases in reactor accidents, containment performance, risk assessment, and severe accidents. The Committee also studies the safety of the fuel cycle, conducts periodic surveys of reactor safety research programmes and operates an international mechanism for exchanging reports on nuclear power plant incidents.

The Sub-Committee on Licensing, consisting of the CSNI Delegates who have responsibilities for the licensing of nuclear installations, examines a variety of nuclear regulatory problems and provides a forum for the review of regulatory questions, the aim being to develop consensus positions in specific areas.

TABLE OF CONTENTS

FOREWORD

With the formation of Principal Working Group 5 at its tenth meeting in 1982. the CSNI gave PWG5 the following terms of reference:

> "To deal with the technology and methods of identifying factors contributing to risk and assessing their importance, and exchange information on current research. The Group will receive input from the four other Principal Working Groups with a view to developing a common understanding of the different approaches to risk assessment now being developed."

The following specific aspects were -- amongst others -- considered by the CSNI as being particularly worthwhile pursuing.

- -- develop a common understanding of the different approaches to risk assessment now being developed, notably of the use of PRA techniques as an aid in safety decision making in the following areas:
  - -- priorities in safety research programmes;
  - -- guidance on the optimisation of plant design, operation and maintenance;
- -- exchange information on national efforts to develop safety goals, and on the use of PRA techniques in conjunction with qualitative safety goals (including preliminary views on the roles of PRA and safety goals in licensing).

At its second meeting in September 1983, PWG5 recommended a "survey of applications made of the results from previous probabilistic risk assessments" as one of three principal tasks for 1984.

In November 1984, the CSNI generally endorsed the Group's proposals for its programme of work and recommended that in its survey of applications made of previous risk assessments, the Principal Working Group should try to assign priorities to the instances where PRAs had an influence on decision making, focussing on practical aspects such as modifications made to design or operation of plants.

In the Introduction to the following review paper the Task Group explains its understanding, approach and working methods regarding the Task.

1. INTRODUCTION

1.1 General remarks to safety decision making and the use of PSA/PRA

The safety management of industrial plants associated with major hazards to plant personnel, or to the public, consists fundamentally of decision making concerning risks. In a great variety of situations it has to be decided whether safety design or operational practices are sufficiently safe or not.

At the beginning of new technological developments, long term operating experience, adequate analytical tools, probabilistic methods and data are not available. Therefore safety requirements are developed by engineering judgement with respect to the state of knowledge in terms of specified technical requirements, e.g. to install specific safety features such as pressure control systems or a certain degree of redundancy in safety systems. In the nuclear field these safety requirements are usually called the deterministic approach to safety.

The basic principles of decision making for nuclear power plant safety are usually laid down in general terms in the mandatory requirements of the respective acts and ordinances. They usually require adequate protection of public health and safety or demand the necessary precautions against damage, according to the established state of science and technology, as a prerequisite for a license to construct or operate a nuclear power plant.

Current regulatory practices are believed to meet the basic statutory requirements. Nevertheless, there are different issues, insufficiencies or limitations where the current practices of investigating and deciding nuclear power plant safety matters can be improved by using the latest advances in safety assessment methods.

Decisions regarding nuclear power plant safety have been based upon a set of generic engineering principles, a defence-in-depth concept, a family of design basis accidents and other regulatory requirements, specific design criteria and operational features for each plant. Some issues of special importance have been decided case by case on the basis of a mixture of engineering judgement, operational experience or political reasoning.

Although not explicitly described or quantified by reliability, risk limitation or other probabilistic requirements, a probabilistic judgement has always been inherent to this decision making process. Moreover, on the different levels of the hierarchy of regulatory requirements, safety rules and criteria very often contain qualitative probabilistic requirements concerning frequencies and consequences of events such as: sufficiently reliable, negligibly small, remote, highly improbable, no unreasonable risk, as low as reasonably achievable (ALARA-principle).

Within this context, probabilistic approaches are more and more accepted. PSA/PRA not only provides an additional technique for assessing the safety of a particular nuclear facility, but also an information base that is applicable to a wide variety of issues and decisions.

There should be a strong relationship between the state-of-the-art of PSA/PRA and the state of successful applications. As the strengths of probabilistic approaches become visible and the limitations of data, methods and experience are reduced and are better understood, more confidence and reliance can be placed upon PSA/PRA. More weight can be given to qualitative and quantitative PSA/PRA insights versus all other available and pertinent information and the former implicit probabilistic approach can be made more explicit and systematic.

The incentive to move to the application of PSA/PRA mainly results from the intention to resolve safety issues in conformity with the following objectives:

-- adequate safety of plant design and operation;

-- well-balanced design, treating safety issues according to their relative importance;

-- risk management throughout the lifecycle of the plants;

-- optimal allocation of resources for improving safety;

-- rational decision making processes.

It is now common to perform at least some reliability analyses of essential systems of nuclear power plants in the course of the licensing procedure. Systematic reliability analysis or probabilistic safety assessments are considered as one of the more important management tools to verify, maintain and improve reactor safety.

1.2 Historical background

About ten years ago the draft version of the Reactor Safety Study (WASH-1400) was published in the U.S.(1). It was the first comprehensive application of probabilistic methods to evaluate nuclear safety and it demonstrated that a nuclear power plant can be analysed in a systematic way by PRA techniques.

In the following years, the merits and limitations of these methods have been discussed intensively and often controversially, amongst experts as well as by a broader public. The controversy on the question as to whether WASH-1400 gave a reasonably trustworthy prediction of the so-called bottom-line societal risk distracted many people from exploring those uses of probabilistic reactor safety studies that would be more trustworthy than such bottom-line predictions.

In 1977 the United States Nuclear Regulatory Commission (USNRC) chartered the Risk Assessment Review Group, known as the Lewis Committee, to review WASH-1400. The committee confirmed (2) that the uncertainties surrounding the bottom-line risk predictions were larger than those identified in WASH-1400 and identified a number of methodological weaknesses in that pioneering venture in probabilistic reactor study. However, the Lewis Committee also endorsed the basic approach and urged more extensive use of probabilistic risk assessment in reactor safety regulations:

-- "We do find that the methodology (of WASH-1400), which was an important advance over earlier methodologies applied to reactor risks, is sound, and should be developed and used more widely under circumstances in which there is an adequate base or sufficient technical expertise to insert credible subjective probabilities into the calculations. Even when only bounds for certain parameters can be obtained, the method is still useful if the results are properly stated. Proper application of the methodology can therefore provide a tool to make the licensing and regulatory process more rational, in more properly matching resources (research, quality assurance, inspection, licensing regulations) to the risks provided by proper application of the methodology." (2)

Nevertheless, others believe that while PRAs do yield numerical estimates and are thus "quantitative", the estimates are so imprecise and subject to manipulation as to be virtually useless in decision making. Given such controversy, it is not surprising that the role of PRA in the regulatory process has not yet been defined.

The similarity of the Three Mile Island (TMI) accident with predicted accident sequences in WASH-1400 and in the German Risk Study (3), justified and accelerated the use of the probabilistic methodology. Based on the reports of the Rogovin (4) and the Kemeny (5) Commissions, the original methodology has been further developed and more widely applied. For that reason the use of such analyses in safety evaluation and decision making in its broadest sense, either as a formal part or, more often, as an informal part, has increased steadily in recent years. So far more than 30 plant-specific risk studies for LWRs have been performed (see Table 1).

1.3 Implementing PRA in the safety decision making process

These studies made evident, for example, that system reliability analysis applied to safety systems of a nuclear power plant deepens the insight into the structure and interaction of those systems and helps identify weaknesses in design. Furthermore, through consolidation of techniques from various disciplines, it became possible using risk assessment techniques to combine viewpoints of many specialists into one coherent picture of reactor safety. This combination of techniques assists in overcoming the major difficulty in analysing a modern nuclear power plant, namely that it is impossible for one person to fully understand the whole plant.

From the experience gained so far it can be concluded that:

-- the application of probabilistic methods to nuclear power plant safety issues offers engineering and safety insights that can only partly be gained by other means;

-- there are nuclear safety issues which can only be assessed properly if they are also analysed and evaluated systematically with probabilistic methods.

However, whilst probabilistic methods have proved to be a powerful tool to investigate a variety of aspects of nuclear power plant safety, they have certain inherent strengths and limitations which make them very useful for some applications while perhaps poorly suited for others. With the better understanding on probabilistic methods and better information on probabilistic data through operating experience, a description of nuclear safety in a more systematic and quantitative way is possible.

In the absence of probabilistic data, e.g. for rare events, the decisions were made by engineering judgement, the so-called deterministic approach. Probabilistic methods can provide a useful complement -- but not a total replacement -- for deterministic approaches.

Therefore, those who are responsible for nuclear safety need to develop a way to integrate probabilistic approaches into the safety decision making processes. As the application to traditional safety criteria and practices have served their purpose well in the past, this means a decision on where and how the probabilistic methods should complement traditional methods. The answer of course, depends very strongly on the specific national situation, e.g. on the status of the nuclear programme or the legal and regulatory framework.

1.4 Status of the international discussion on PSA applications

The two main approaches for introducing probabilistic methods into the safety decision making processes are the political, normative approach and the technical, pragmatic approach. These two approaches are discussed briefly below.

1.4.1 The political, normative approach

Concern that reactors might pose a disproportionate societal risk promoted attempts to measure this risk so that it could be compared with other risks that are considered to be acceptable. Since absolute safety is not achievable, the question of "how safe is safe enough" was raised.

Probabilistic safety goals have been developed and discussed in several countries. These goals are intended to give a distinct and practicable measure of acceptable risk (6, 7, 8).

1.4.2 The technical, pragmatic approach

It has been recognised that the probabilistic approach allows not only quantification of system reliability, but also identification of systems interactions and plant safety design imbalances. Insights gained have often stimulated changes of design or operational procedures. A growing interest in taking advantage of the insights offered by probabilistic safety assessment is evident in many countries (9, 10).

Because of the increasing application of probabilistic techniques, procedures have been created to give guidance on PRA methods (11, 12). Besides these activities, much literature has been published with different proposals or concepts regarding how to apply lessons learned from PRA to nuclear safety issues.

Table 1: Risk Studies for LWRs Completed or Underway

Country	Plant	Type	Rated Power MW	Containment	Nuclear System	Operating License	Study Issued	Sponsor
Canada	Darlington	PHWR	4 x 850			1977/80	(1988)	Utility
Finland	Loviisa 1 & 2		2 x 440					
	Olkiluoto I & II		2 x 660	Approx. Mk.II	ASEA	1978/79	(1988)	Utility
France		DWR	900				(1988)	Utility
F.R. of Germany	Biblis B	P	1300	Dry sphere	KWU		1979	BMFT
Italy	Alto Lazia	B	2 x 1000		Ansaldo,		1984	Ansaldo
	PUN	P			GE/EBASO NIRA/W			Utility
Spain	Santa Maria de Garona							
Sweden	Ringhals 2	B	860		W		1983	NUS/SSPB ASEA
Switzerland	Leibstadt	B	1000	Mk. III	GE		1984	
	Goesgen	P	970		KWU		1984	
	Beznau I/II		2 x 350		W		(1985)	Utility
United Kingdom	Sizewell B	P	1100		W/NNC		1982	
United States	Arkansas One 1	P	858	Dry	B&W	1974	1982	NRC(IREP)
	Big Rock Point	B	75	Dry sphere	GE	1962	1981	Utility
	Browns Ferry	B	1067	Mk. I	GE		1982	NRC(IREP)
	Calvert Cliffs 1	P	845	Dry Cyl	CE	1974	1981	NRC(RSSMAP)
	Calvert Cliffs 2	P	845	Dry Cyl	CE	1974	1983	NRC(IREP)
	Crystal River 3	P	845	Dry Cyl	B&W	1976	1982	NRC(IREP)
	Grand Gulf 1	B	1250	Mk. III	GE	1982	1981	NRC(RSSMAP)
	Indian Point 2	P	873	Dry Cyl	W	1973	1982	Utility
	Indian Point 3	P	965	Dry Cyl	W	1973	1982	Utility
	Limerick 1, 2	B	1055	Mk. II	GE	(1985)	1983	Utility
	Midland 2	P	805	Dry Cyl	B&W	cancelled	1984	Utility
	Millstone 1	B	652	Mk. I	GE	1970	1983	NRC(IREP)
	Millstone 3	P	1156	Dry Cyl	W	(1980)	1983	Utility
	Oconee 3	P	860	Dry Cyl	B&W	1973	1983	NRC(RSSMAP)
	Oyster Creek 1	B	620	Mk. I	GE	-	-	-
	Peach Bottom 2, 3	B	1098	Mk. I	GE	1973	1975	NRC
	Sequoyah	B	1148	Ice Cond	W	1981	1981	NRC(RSSMAP)
	Shoreham	B	820	Mk. II	GE	(1984)	1983	Utility
	Surry 1, 2	P	824	Dry Cyl	W	1972	1975	NRC
	Susquehana 1, 2	B	1100	Mk. II	GE	1983	1983	Utility
	Yankee Rowe	P	175	Dry Sph.	W	1960	1982	Utility
	Zion 1, 2	P	1100	Dry Cyl	W	1973	1981	Utility
	Seabrook	P	1150	Dry Cyl	W	(1984)	-	-
	Ozonee 3	P	792	Dry Cyl	B&W	1973	1981	EPRI/NSAC
	Gessar II	B	1269	Mk. III	GE	None	1984	GE

0975Y

In practice the use of PRA as a technical, pragmatic approach is far more evident than its use as a political, normative approach.

1.5 Approach and methods of PWG5/Task 2

A main task of CSNI PWG5 is to synthesise technical understandings and consensus opinions based on detailed results from task-oriented, short-term activities.

Concerning Task 2, this means:

-- to review all work on PRA/PSA applications;

-- to assemble a collection of case studies where PRA methods and results had an influence on safety decision making.

The best way to use PRA techniques as an aid in safety decision making depends on the specific situation, e.g. the specific lines of formal responsibility and the process of decision making used in different nations.

Evaluation of technical literature has been considered to be inappropriate for that purpose, since the literature is typically too inhomogeneous and too theoretical and it does not necessarily reflect the true state in which these techniques are applied. The need for a better and more reliable information base has been recognised. Therefore, the work of this Task Force has been based mainly on a compilation of examples that demonstrate concrete practical experience with the application of probabilistic methods in reactor safety decision making.

2. FUNDAMENTALS OF THE PROBABILISTIC APPROACH

2.1 Terminology

The following terminology and definitions have been adopted as far as possible from IAEA TECDOC-308, Reliability Analysis and Probabilistic Assessment in the Licensing of Nuclear Power Plants.

2.1.1 General Terms

Probabilistic approach (in contrast to the deterministic approach): use of logic structures (event trees and fault trees) and analytical techniques (models of systems and processes) to estimate expected frequency and consequences of certain events in order to obtain a unified and comprehensive description of events to which the plant might be subject.

Probabilistic Safety Analysis (PSA): a study of whatever scope that includes a probabilistic approach to safety analysis.

Probabilistic Risk Assessment (PRA): PSA extended to compute a "bottom line" risk in terms of the offsite radiological risk posed by potential reactor accidents. Results are often displayed by means of complementary cumulative density functions (CCDF).

2.1.2 Levels of PSA

Levels 1 to 4 cover the analysis of systems and plant behaviour; levels 5 to 8 cover the analysis of accident consequences.

Level 1: Reliability evaluations for protection and safety related systems. The objective is to predict the probability that each system will fail to perform its safety function on demand.

Level 2: Assessments of the conditional probability that the design basis of the plant will be exceeded, assuming that a specified initiating fault, fault sequence, or group of faults has occurred. This is a big step beyond Level 1 and account must be taken of all interactions among systems.

Level 3: An assessment of the frequency that the design basis for the NPP as a whole will be exceeded. This assessment is done by adding up the frequencies for the various faults, as in Level 2, over the whole range of possible faults. The concern here should be to ensure completeness in the coverage of faults, with no omissions or overlaps.

Level 4: An assessment of the frequency of severe core damage, core melt, or large-scale core melt.

Level 5: An assessment of the frequency distribution of the radioactivity released, expressed for example in Equivalent Curies of I-131. This type of study requires further phenomenological calculations concerning modes of containment failure, their timing, and the transport of radionuclides from the damaged core to the environment.

Level 6: An assessment of the resulting expected radiation dose to an individual member of the public. Usually this means assessing the frequency with which the person most at risk will receive a dose in excess of a specific level.

Level 7: The results of Level 6 above expressed in the form of a dose/frequency distribution, combined with a dose health effect relationship and integrated to predict the frequency of death from the dose for the individual most at risk. This is usually presented separately for early (acute) fatalities and late (cancer) fatalities.

Level 8: An assessment of the overall health effects on the total population that might be affected. The results are usually presented as curves showing the complementary cumulative frequency distributions for early and late fatalities.

These definitions are useful for discussing scope and depth of PSAs, but they do not cover all aspects, as, for example, interfacing system LOCA.

Another convention for levels of analysis that is widely used in the U.S. originated in the ANS/IEEE PRA Procedures Guide (NUREG/CR-2300). As used in that document, Level 1 corresponds with Level 4 above, although only for internally initiated events; Level 2 corresponds most closely with Level 5 above; Level 3 corresponds with Level 8 above; Level 4 also corresponds with Level 8 above, but includes not only internal accident mechanisms but also external events such as earthquakes, fire and storms as accident initiators.

2.2 The respective roles of deterministic versus probabilistic analyses versus evaluation of operating experience

In the following discussion, we mean to exclude decisions such as:

-- the fundamental (positive) decision to use nuclear energy;

-- the general decision that nuclear power plants can be built and operated at an acceptably safe level.

These questions have been decided by political, economical and social aspects in each country. We mean to address questions of safety arising in aspects of design, licensing and operation. In deterministic safety analyses, accidents are postulated a priori, and the plants have to be designed in order that these accidents do not cause unacceptable consequences. Reliable operation of safety systems, when called upon, is assured by applying deterministic safety principles (e.g. redundancy, diversity).

This concept is verified and corrected by operating experience as well as by probabilistic safety analysis.

The probabilistic assessment helps:

-- to better understand the safety characteristics of a plant;

-- to optimise plant design and operation;

-- to anticipate "experience" which otherwise would have to be gained by negative operating experience;

-- to explore the vulnerability of the plant to accidents more severe than the design basis accidents.

Strengths and weaknesses of all three elements of safety evaluation are indicated in Table 2.

2.3 Main problems in deciding whether to adopt a probabilistic approach and how to implement it

Whether, and in which way, a probabilistic safety analysis should be performed may depend on a number of circumstances. Conditions that should be considered are described below.

1. Is the use of PRA/PSA obligatory?

   In some cases PRA/PSA has been made obligatory by licensing authorities. However, up to now this does not seem to have become a common practice. In most cases, PRA/PSA is seen as a supplement to the formal, deterministic approach to reactor assessment.

Table 2

Approach	Strength	Weakness
Deterministic	Plain and easily applicable Simple to check Provides inherent safety and reliability features is less sensitive according to incompleteness	Safety design may not be well balanced Overall level of safety not quantified Subjectiveness of assumptions Offers no information about necessary test intervals
Probabilistic	Provides integrated plant model Allows ranking of safety issues and balancing of safety design and system modifications Uncovers design weakness Optimise test, inspection and maintenance procedures Quantification of operating experience	Inherently incomplete High costs for detailed analysis Probabilistic data base is necessary Probabilistic models need to be simplified, therefore, subjectiveness of assumptions Need for specially trained expert teams
Evaluation of operating experience	Direction quantification of component and system reliability Human influence and CCFs directly perceptible Feed back of operational experience is possible	Few experiences with "rare events" Experiences cover only part of safety aspects No information about the effects of system modifications

2. To which criteria should respective safety goals be applied?

Before starting a PSA it should be clear which criteria should be used to assess the safety of a plant. The formulation of the criteria may strongly influence the approach to be chosen for the PSA. On the other hand, PSA can be used very effectively even in the absence of quantitative probabilistic criteria, e.g. to look for weak points in systems design.

3. How much manpower and other resources are available?

The available manpower and the level of funding will determine the comprehensiveness and the degree of detail of a PSA. If resources are limited, a decision must be made whether to perform either a thorough analysis of smaller scope or a wide-ranging but cursory study.

4. Are plant owners co-operative?

If a real plant instead of a plant concept is to be analysed, co-operation with the organisation operating the plant is very important. A reliable PSA needs a lot of information that can best be gained from operating experience, detailed plant documents, and visits to the plant. Fortunately, the understanding is growing that PSA can be very valuable to the plant owner/operator.

5. Are details on plant design available?

A detailed PSA requires detailed knowledge about how the actual plant is constructed. This information is usually available for completed plants. If a PSA is to be performed for plants which are still under construction or even in the design phase, a higher number of subjective estimates must be used.

6. Is the plant design unique?

PSA, even for specific plants, can profit from analyses performed for similar plants. For instance, frequency of initiating events can be better estimated if a larger amount of operating experience with the same type of plant is available. On the other hand, generic experiences may not be truly representative of the plant in question. In the treatment of uncertainty it should be recognised that the data base drawn from a large population of plants may misrepresent the reliability of equipment or operators in the particular plant.

2.4 Application of PSA/PRA information and insights

The establishment of a PSA/PRA model of a plant entails integration of the contributions of many specialists: mechanical, electrical and control system design, provisions for test and maintenance, procurement specifications and equipment qualification, start up testing and procedures and schedules for surveillance as well as operation. These plant models have been used:

-- to evaluate alternative design changes, to plan and review modifications of the plant or of operational procedures. Very often a relatively straightforward and cheap design change, such as adding a redundant valve or reducing a test interval can improve the reliability or availability of a certain safety feature significantly. This is considered as a strong reason for carrying out at least a simplified PRA at the design stage;

-- to evaluate operational experience, to assess the safety significance of occurrences for the plant or applicability to other plants;

-- to train plant personnel in safety systems functions and their interdependencies in order to increase understanding and awareness of plant behaviour.

As higher level PSA/PRA treats the entire plant and its constituent systems in an integrated fashion, it cuts across traditional lines separating the various design and operational disciplines. Instead of analysing certain event sequences under given initial and boundary conditions, a PRA propagates faults across design interfaces or boundaries. This makes it possible to distinguish between safety issues with regard to their relative importance. Therefore PSA/PRA results and insights have been used:

-- for specific application of the deterministic approach to safety consisting of design basis accidents, design principles and conservative assumptions;

-- to identify safety issues and establish action priorities to improve overall plant safety. PSA/PRA reveal plant features -- weak points -- that may merit closer attention and provide a focus for improving safety;

-- as a guide to ensure that all measures of the overall reactor safety concept are well balanced;

-- to analyse new safety issues as they arise for operating or planned power plants.

While the applications listed above can be used to optimise plant design and operation within or close to the actual design basis, PRAs trace event sequences even beyond the design basis to estimate severe accident consequences together with likelihoods. The information base provided by the analyses has been used:

-- to indicate the actual level of nuclear power plant safety by introducing quantitative safety indices and measuring safety margins beyond the design limits on a best estimate basis as a reference for future safety decisions;

-- to focus resources on efforts to reduce severe accident risk, on preventive and mitigative features most important to safety and to exploit maximum technical control over the initiation and progression of events that may lead to severe accidents;

-- to develop strategies for coping with accidents beyond the current design basis, i.e. to identify possibilities of diagnosing the most probable severe accident sequences, to provide information and guidance to the operators to deal with such accidents, and to provide information for developing emergency response plans.

The information base provided by PSA-PRA approaches described above gave further guidance for research and development:

-- to evaluate new safety concepts for power plant development as necessary;

-- to develop long-range research programmes and to assign priorities to generic safety issues;

-- to uncover safety issues potentially new to the industry;

-- to define objectives and technical boundary conditions and specifications for certain research activities;

-- to describe and evaluate possible safety improvements achievable by the application of safety research results.

Growing use of PSA/PRA results and insights have been made in the regulation of nuclear power plants:

-- as a guide to regulatory standards development; for example to assist in formulating new regulatory requirements, to reassess existing requirements or to eliminate or reduce requirements on issues not important to safety;

-- to evaluate regulatory compliance by setting limits to failure rates, systems availability or reliability, core damage frequencies or frequencies of doses;

-- to evaluate the urgency with which backfits must be implemented or to set in-plant priorities for backfits;

-- to developing siting criteria;

-- to develop emergency plans.

Finally, the information compiled by the different probabilistic approaches to nuclear power plant safety has played an increasing role in political discussions, public hearings, discussions with intervenors against certain projects or in court actions. In all these cases, PSA/PRA information was used as another point of view to assess the adequacy of nuclear power plant design and operation.

In general PSA results have two distinct benefits:

-- to provide a systematic framework for communication of safety performance information to parties involved in decision making;

-- to evaluate engineering aspects of complex systems.

In decision making, both aspects of PSA results are involved.

3. REVIEW OF THE REPORTS ON PRACTICAL APPLICATIONS

3.1 Organisation of the review

The purpose of this report is to survey past and present applications of PRA methods and results in safety decision making processes by assembling a collection of case studies where PRA methods and results have had an influence on decision making, e.g. regulatory changes, licensing requirements, plant specific modifications, modifications in plant operation, emergency planning, alteration of safety R&D programmes, etc.

Using delegates answers to the very broad study "Survey: PRA Historical Perspectives" [SINDOC(84)166], the Task Group prepared a questionnaire on applications, produced from methods and conclusions of previous PRAs.

This questionnaire was intended to compile practical experience that has been gained in applying the insights and results of probabilistic safety assessments to safety decision making related to nuclear power plants. Examples are sought not only involving comprehensive PRAs, but also other types of probabilistic safety analyses (PSA). Of highest priority are instances where the probabilistic approach made a major contribution to resolving important safety issues, particularly to practical aspects such as modifications to plant design or operation. Both positive and negative experience is of interest.

The information collected was reviewed with a view to identifying promising areas of application and procedures by which the probabilistic viewpoint can provide useful input into decision making processes.

Grouping of the survey results was based on the responsibilities of the different parties interacting in the decision making processes. Usually more than one party is involved:

-- design industry and utilities;

-- regulatory authorities and their experts;

-- research institutions.

The information requested in the questionnaire made it possible to categorise the applications collected in several ways, e.g.:

-- decision making areas in which PSA results were applied;

-- criteria applied in the decision making process;

-- type of plant [or system(s)] and stage of its "life cycle" at which the PSA used was carried out;

-- affiliation of the study team;

-- level of probabilistic safety analysis carried out.

The following sections provide generic insights on the experience documented by the survey. These insights are intended to support general conclusions about further actions and limitations concerning additional uses of PSA for decision making. Regulatory activities encouraging or requiring certain PSA/PRA applications, particularly, should not only depend on the state-of-the-art of the methodology, but also on the extent of applications by other parties involved.

The results of the review were categorised as follows:

-- optimisation of plant design and operation (within the design base);

-- regulation;

-- special safety aspects and problems;

-- safety research and technological development.

3.2 Optimisation of plant design and operation (within the design base)

As can be seen from Table 3, application of PSA/PRA for optimising plant design and operation is frequent, particularly in European countries. Sometimes it is difficult to distinguish between this type of application, where the decisions are taken by a vendor or a utility, and applications where PSA/PRA are used in regulatory activities (see Section 3.3). This ambiguity results from the fact that usually the licensing authorities must at least agree with the decisions. In most cases they are even involved in the process of initiating and performing the PSA. It should be noted that none of these applications is intended to be used to prove compliance with formal criteria as in the development of formal criteria.

Probabilistic methods can be applied in optimising plant design and/or operation for different reasons and purposes:

-- to assist in making decisions about plant design and operation:

In solving a special problem concerning detailed plant design, a vendor may feel that a probabilistic assessment is necessary to find the best solution with respect to plant operation and safety. For example, post-accident operating procedures or maintenance and test intervals may be optimised in this way.

-- to determine adequate reliability of system functions:

Reliability analyses of systems may be requested by licensing authorities for conditions that are usually not considered in terms of deterministic rules. There might be an indication, for instance, that an improvement is possible by simple means. (Aus 2, Aus 3, Ger 1, Bel 1, Bel 2, Spa 1).

-- to determine compliance of plant design and operation with established criteria:

Formal criteria may be vague. For example, only a "sufficient reliability" may be requested for some safety functions. In this case, probabilistic methods may be used to show that the intent of the respective criteria is met. The same holds if a specific

<u>Table 3</u> <u>Classification of Applications of PSA</u>
<u>(Secondary Applications are in Parentheses)</u>

Area of Application	Level of PSA 1	2	3	4	5	6	7	8
Optimisation of plant design and operation within design base	Aus 2	Ger 3	Ita 1	Ita 2	Ger 6			Can 1
	Aus 3			Swe 1				Ger 10
	Bel 1	Fra 1		Swe 2				USA 5
	Bel 2	Ger 7						
	Ger 1	Ger 8						
	Spa 1	Ger 9						
Special or new safety issues		USA 4		Ger 7		UK 1		
Regulatory activities	Bel 3							
	Ger 2		Ita 3	Ita 4	Ger 5	Aus 1		Ger 11
		Swe 3		Ita 5		Ger 4		USA 2
	Aus 2	USA 8		Ger 9		Swi 1		USA 3
	(Aus 2)							USA 6,7
	(Aus 3)							USA 9
	(Bel 1)	(Fra 1)						USA 10
	(Bel 2)							USA 11
	(Bel 3)							USA 12
	(Ger 1)							
Safety research and technological development					(Ger 6)			USA 1

application of deterministic rules is favourable, i.e. if the formal application of a combination of deterministic requirements would lead to unrealistic or excessive demands concerning extremely unlikely events. (Ger 3)

-- to evaluate plant design:

For various reasons, a complete PSA of a plant design may be conducted either by a vendor or by some other institution. These reasons can include requests or recommendations by the licensing authorities and the desire of a vendor to show that a new or existing plant design is well-balanced and comparable to other designs. During such an analysis, some design deficiencies may be revealed and rectifying action initiated. (Can 1, Ger 5, Ger 6, Ger 7, Ger 9, Ita 1, Ita 2, Swe 1, Swe 2, USA 5).

The effort which is necessary to solve problems of optimisation by probabilistic methods depends on how diffuse a task is established. An advantage of this type of application is that to a large extent Level 1 or 2 PSAs are sufficient to solve special problems. In most cases only one person/year or less is required. If a complete PSA is conducted for a whole plant to detect the weak points, the effort is typically in the range of 20 to 50 person/years. When a weakness in design is revealed it may be necessary to make a more detailed Level 1 or 2 analysis for that special problem, but rectifying deficiencies usually seems to be possible in an uncomplicated and low cost way.

As far as the answers to the questionnaire are concerned, experience tells us that for this type of PSA application the decision making process is quite straightforward. The purely technical character of the problems and the absence of formal or inflexible rules in fact facilitate the decision making process. The advantage of a certain alternative system design or operation mode is usually quite obvious. But even if the costs of certain backfitting measures are not negligible, it will usually not be difficult to take a reasonable decision on the basis of the results of the PSA and engineering judgement.

As has already been mentioned, licensing authorities or their advising experts usually take part in the decision making process. This procedure has proved quite successful.

In the answers to the questionnaire, essentially positive comments were given to the kind of PSA application discussed above, for instance:

-- a major advantage of PSA is the insight gained into a system that results from a disciplined and structured analytical approach. For this reason the design should be closely associated with the analysis. (Aus 2);

-- the process of system modelling can provide a useful information base on which to develop post-accident operating procedures. (Can 1);

-- by using the probabilistic approach, an improvement of systems reliability and a simplifying effect to licensing were achieved. (Ger 1);

-- the results of probabilistic safety analyses were very helpful in developing the new safety concept of HTR-500. (Ger 6);

-- a problem area was revealed as a result of the systematic and detailed analysis of system functions that is part of PSA studies. Although the same result might, in principle, have followed from an analysis emphasising deterministic criteria, our experience suggests that comprehensive and thorough PSA analysis is a valuable check of traditional safety assessments. (Swe 2);

-- this application demonstrated the value of a plant specific PRA to the performing utility. The PRA identified the dominant accidents at the plant and cost-effective changes that could be implemented to reduce the plant risk. (USA 5).

Only a few negative comments were provided, such as:

-- application of PSA is limited because of the difficulty in quantifying dependent faults and obtaining applicable failure rate data. (Aus 2);

-- it is difficult to obtain consensus between analysts and designers on the necessary level of defence against dependent faults. (Aus 3);

-- the benefits indicated by PSA are strongly analyst dependent. (Can 1).

3.3 Regulation

Regulatory applications of PSA have been completed as supplements to traditional deterministic methods. The belief stated in the survey responses is that deterministic methods have been successful in assuring an adequate level of safety in nuclear power plants. PSA offers a different viewpoint that can be useful in refining the current regulatory philosophies. Goals that lead to these applications can be divided into four types:

1. assuring that additional requirements provide a significant safety gain;

2. plant specific improvements are possible by virtue of the application of a PSA, i.e. to achieve a well balanced safety design (Ger 13);

3. review of existing requirements is needed to maintain their effectiveness;

4. control of severe accidents.

Use of PSA for new regulatory requirements has been applied at several levels of influence in the regulatory structure. These levels range from general policy to modifications to specific systems. Examples include the following:

-- formal review of all new regulatory requirements (USA 9), value impact assessments (NUREG/CR-3568);

-- develop a severe accident policy (NUREG 1090, SARPP);

-- rulemaking concerning special safety issues: ATWS-rule (USA 7);

-- interpretation of the application of single failure criteria in connection with external events (Ger 11).

These applications all have the goal to quantify a significant safety benefit for the required actions. In addition, U.S. applications apply cost effectiveness criteria for items with moderate safety benefits.

There are two main motivations for regulations requiring the completion of PSAs. These include the need for additional studies to expand the regulatory data base and to provide a motivation for plant operators/designers to obtain plant-specific insights about potential weaknesses in design and/or operations. The identified weaknesses can result in improvements in the plant that would not have been covered by generic regulatory actions. Specific reasons for requiring PSA studies include:

-- to review plant designs in the initial licensing stage by requiring a PSA/PRA together with other licensing documents, e.g. for Standard Plant Designs;

-- to assess if the plant design is well balanced (no outliers) (Ger 13);

-- to assess safety improvements compared to former plants (Ger 5);

-- to allow a probabilistic differentiated application of deterministic principles (classification of design basis events according to their expected frequencies) e.g. UK-NII -- safety assessment principles;

-- to demand periodic reassessments of plant safety on a probabilistic basis (Systematic reliability assessment, PSA) using plant specific "as operated data" (Swedish ASAR, plant specific precursor studies).

Reassessment of existing safety requirements is an ongoing process to assure that safety levels are maintained in the light of new operating experience, advancements in technology and the addition of new requirements that may supersede or overlap with the old. PSA, as in the case of new requirements, can offer new perspectives on existing requirements that have a largely deterministic basis. Specific actions have been carried out in the areas of siting, backfits, emergency planning, public hearings and court actions.

Backfit decisions are similar in scope to those made for new requirements. They involve the application of existing regulations to older plants. The U.S. Systematic Evaluation Program (USA 2) has made detailed comparisons of existing regulations and those used in the licensing of older plants. Items have been selected for backfit based on their improvements in safety and cost effectiveness.

Emergency planning can be completed on the basis of PSA results. The advantages of this approach include the option of selecting from a variety of reference accident scenarios for planning emergency responses (Swi 1). PSA results have also been used to establish emergency planning zones (USA 6).

PSA results have been used effectively for discussing public safety in legal enquiries. This includes the comparison of PWR and other reactor designs in the Sizewell B hearings and hearings on Indian Point safety in the U.S. (USA 3). The Federal Republic of Germany courts considered PSA results in a determination that nuclear power plants provide adequate protection to the public (Ger 13).

Control of severe accidents has led to the development of probabilistic criteria for safety systems and overall plant performance. These criteria are used as a supplement to deterministic rules for the prevention and mitigation of severe accidents. Examples from the survey include:

-- UK-NII safety assessment principles;

-- French PWR Safety Goals;

-- other national "safety goal" approaches: e.g. Canada, Italy, Switzerland;

-- numerical reliability goal for AFWS (USA 8);

-- numerical criteria for design against aircraft crash (Bel 3).

The bases for these criteria include the historic reliability of similar systems, availability of new technology to improve reliability and judgment as to a tolerable level of equipment failures. The historic basis for probabilistic criteria is to limit the possibility of unacceptable consequences (exceeding design basis). Reliability criteria serve as a complement to the single failure criteria for systems that, because of technology limitations, must make use of less reliable components. In more recent applications, reliability criteria have been based on values used in PSAs to limit the risk contribution of a particular system. This example represents an extension of judgement in identifying equipment that is important to safety and supplements single failure rules.

Specifying probabilistic criteria for safety system design and function has been a regulatory approach in the U.S. The results of PSAs are directly applicable to engineered systems, and analytical methods are sufficiently mature to allow independent verification. This level of decision is directly related to equipment performance and encourages the use of PSA techniques early in the design process to optimise safety and operability.

Regulation of safety systems using reliability criteria has two major drawbacks: the process of setting criteria for particular systems is judgemental and there is relatively little encouragement for innovation in the combination of plant systems. Setting reliability criteria for particular systems without an assessment for the entire plant can possibly result in requirements that are inconsistent with the safety importance of those systems. Limitations based on existing systems may not encourage innovations in systems where new technologies are available. Incorporation of new system designs could reduce requirements in other safety systems and maintain levels of safety.

Reliability calculations are partially motivated by safety regulations. Thus, design decisions that enhance both plant operability and safety are accommodated at an early stage of system engineering. This type of decision is discussed in Section 3.1. Additional decisions related to multi-system design take place when larger scale PSAs are completed. The UK and FRG concepts of limiting contributors to plant accident sequences created the needs for PSA, additional design reviews and communication of the results to regulatory authorities for review. These overall plant reliability requirements are an extension of reliability requirements for individual systems.

3.4 Special safety aspects and problems

PSA-based decisions related to special problems can be defined as a combination of the first three categories of decision. These decisions are comprised of items that are technically complex, involve many plant systems, and are of sufficient safety importance that regulatory action is taken concurrently with development of technical solutions. Examples of special safety aspects and problems in the U.S. include pressurised thermal shock, Three Mile Island accident response, and degraded core rules.

The TMI accident revealed that perhaps reactors were not "safe enough", that the regulatory system had some significant problems (as cited in both the Kemeny and Rogovin investigations), that the probability of serious accidents was not vanishingly small, and that new approaches were needed. Suddenly, the potential value of PRA as a regulatory tool -- and of the insights of the RSS itself -- became apparent to the reactor safety community.

People observed that the RSS had found transients, small loss-of-coolant accidents (LOCAs), and human factors to be dominant contributors to the overall risk and that the TMI 2 accident sequence contained all three of these.

Different systematic failures in high redundance safety relief valve systems have been discussed in the FRG and in the Netherlands. PSA was used for analysis and to assess if these systems needed improving. The following activities are usually involved in the resolution of special problems:

1. evaluation of the scope and importance of the problem;

2. development of interim rules for continued operation;

3. research short and long term solutions;

4. modification of short term rules;

5. development of rules for long term solutions;

6. implementation of resolutions.

Use of PSA can be beneficial during each of these steps and is being increasingly applied as an integral part of special issues studies. Since many of the activities are carried out simultaneously, there is a need for effective communications and continuous evaluation of progress. PSA models can be continuously updated to reflect new information and monitor progress.

If during operation of a nuclear power plant significant new safety problems arise, then at first a decision is needed on whether to allow continued plant operation. This decision can be facilitated by the application of PSA models and conservative assumptions to make estimates of safety importance. The results from relatively simple calculations that are required can provide support in establishing interim rules for operation. Interim rules are usually deterministic in nature because of the need for rapid action.

Guiding research for developing short and long term solutions is similar to resolving smaller technical problems. The results of this research must be communicated to those involved in the regulatory process. PSA results are usually refined during this step in order to reduce the conservatism initially applied, to utilise new information that has been made available and to include comparisons to other problems modelled in PSAs. These refined results can be used to guide the development of effective resolutions for a problem and can lead to modification of initial rules.

Once long-term solutions are identified, PSA plays an integral role in reviews prior to rulemaking. Comparisons are made with other problems, and judgements are made to assure that costs are not excessive. The proposed solution must be shown to be effective in controlling the risks presented by the special issue.

3.5 Safety research and technological development

Research/scientific decisions using PSA can be divided into two major categories: evaluation of new problems as they arise and evaluation of possible solutions to existing problems. Decisions based on the use of PSA have been made in both of these areas.

Evaluation of new safety-related problems as they arise is needed to assist in allocation of regulatory resources and research budgets. In making these decisions it is desirable to eliminate items with little safety importance and items that are more efficiently resolved as part of other safety issues. PSA and cost analyses are being used in the U.S. for the purpose of resolving generic safety issues. As part of this process, it is necessary to speculate as to the resolution of an issue. Potential safety benefits and costs can then be evaluated. This speculation forces the thoughtful organisation of the problem for possible study, the gathering of all available information, and an understanding of related work. The practice in the U.S. has been to use existing PSAs for the purpose of evaluating new problems to a practical extent in order to obtain a sufficiently accurate measure of safety importance to allow allocation of minimal resources. In the U.S., principal benefits resulting from prioritisation of safety issues have been that important assumptions made in quantifying risks were displayed and uncertainties were estimated. These benefits represent an improvement over the traditional use of judgement in evaluating safety importance. One limitation of the technique is that issues dealing with items not specifically modelled in PSAs (i.e. human factors) must be subjectively quantified.

Evaluation of solutions to safety problems has the purpose of guiding investigations of resolutions, providing measurements of safety effectiveness of alternative solutions and a basis for subsequent regulatory action. Investigation of resolutions involves the identification of areas of uncertainty and impact on plant safety systems. Areas of uncertainty can be addressed by additional research. Interactions with other plant systems can be described to avoid adverse performance impacts. Integration of PSA with safety research can be used to prevent diversion of attention to side-issues, to co-ordinate the efforts of multiple working groups and to provide continuous feedback on the value of continued research in the area. After alternative solutions are developed to a level of detail sufficient to support a decision for implementation, they can be evaluated in terms of their effectiveness in achieving the desired safety improvement and associated costs. Effective resolutions can then be recommended for implementation.

Regulatory action can result from scientific/technical research. Documentation of safety benefits can be used to determine the importance of continued funding during the life of the project and the advisability of implementing the resolution. PSA can provide a consistent set of information for:

-- prioritisation of NPP Safety Issues (USA 1);

-- prioritisation of Safety Research (NUREG/CR3447);

-- development of new plant concepts with specified risk profiles.

4. SUMMARY AND CONCLUSIONS

The main objectives of this report are:

-- to develop a common understanding of different approaches to the use of probabilistic safety assessments to nuclear power plants;

-- to survey past and present applications of PSA methods and results in safety decision making;

-- to identify promising areas for useful applications;

-- to provide a technical information basis for decision makers on how to implement probabilistic approaches in safety decision making processes.

It is commonly accepted that PSAs/PRAs have emerged as a powerful investigative tool for nuclear safety, and as an additional engineering viewpoint for safety assessment and decision making.

Applications of methods and results of PSAs/PRAs have experienced increasing use and more confidence and reliance have been placed upon probabilistic approaches as models, methods and data have been improved.

There is good agreement about the effectiveness of the use of fault trees and event trees to analyse and describe the efficiency of complex safety systems and different initial events and boundary conditions as well as the possible plant responses under accident conditions.

Concerning very rare or unknown phenomena or events, probabilistic approaches suffer from similar limitations as the traditional approaches to safety decision making.

The actual state of the implementation of probabilistic approaches is different in the Member countries according to the specific national situation. This ranges from qualitative statements to make adequate use of quantitative reliability analysis up to quantitative safety goals. Between these extremes many different levels of implementation are practised.

4.1 Generic results

In general the main advantages seen in the PSA/PRA approach are:

-- explicit description of the level of safety achieved by specific design or operational features;

-- identification of plant vulnerabilities or design weaknesses for the improvement of nuclear power plant safety.

From the experience reported it can be concluded that:

-- the application of probabilistic methods offers engineering and safety insights that can only partly be gained by other means;

-- there are nuclear safety issues which can only be assessed properly if they are also analysed and evaluated systematically from a probabilistic point of view.

While traditional safety decision making -- mainly based on deterministic requirements -- ensures adequate protection of the public, the applications of PSA/PRA results and insights have to supplement this approach for further optimisation of nuclear power plant reliability, operability and safety, especially:

-- for specific applications of deterministic rules;

-- to resolve safety issues according to their relative importance;

-- for proposals to depart from existing rules or practices where the burden of proof rests with those proposing to depart.

Quantitative criteria give guidance on generic issues, but public risk for example is only one of many relevant decision criteria.

Formal quantitative probabilistic decision criteria in general are not needed for plant-specific decision making.

Optimisation of overall NPP performance is a multicriteria decision problem, which must be analysed and solved in the plant specific context.

The multi-barrier and defence in depth concept are not only necessary for adequate protection but also are an appropriate approach to reduce complexity and effort of the multi-criteria decision making processes to optimise overall plant performance by probabilistic methods.

4.2 Useful Regulatory Applications

Positive experience with the use of probabilistic approaches have been reported:

- -- as a guide to regulatory standards development;
- -- on specific applications of deterministic principles (classification of design basis events according to their expected frequencies);
- -- to demand periodic reassessments of plant safety on a probabilistic basis using plant specific "as-operated" data;
- -- as supplementary information for licensing purposes;
- -- to establish probabilistic "safety assessment principles" or quantitative design or safety goals.

Different drawbacks of fixed reliability or other absolute probabilistic criteria have been pointed out. The plant specific context is in general necessary for decision making.

Further applications that have been reported:

- -- backfitting decisions;
- -- emergency planning.

4.3 Useful applications for optimisation of plant design and operation (mainly within design base)

Plant specific systematic reliability analysis, probabilistic safety analysis or low level PRA are considered as important management tools to maintain and improve overall plant performance during all phases of the plant's lifecycle.

Positive experience reported concerns mainly:

- -- conceptual or detailed plant design;
- -- supplementary analyses during licensing procedures;
- -- plant-specific evaluation of operational experience or other new information.

Licensing authorities or their advising experts in general accepted this approach.

Many exceptional positive comments have been stated, negative comments concern known problems such as dependent faults, data availability, analyst-dependence of results, human factors, completeness.

4.4 Conclusions

Taking actual limitations of PSA/PRA methods -- data and resources -- as well as ongoing research, especially source term research, into account, the following conclusions are drawn for the further development of adequate approaches to systematic PSA/PRA applications during the plant's lifecycle:

1. development of a common technical understanding and of principles for a stepwise implementation of probabilistic approaches into the regulatory practice:

   -- principles and methods for the ranking of initial events and event sequences and for the assignment of safety limits and performance criteria for design purposes;

   -- approaches, methods and criteria for the selection and analysis of event sequences and safety functions which can be considered as representative of "sufficient reliability" and "well balancedness" for design and licensing purposes;

   -- principles and approaches to the review of safety requirements against new information.

2. Development of a common technical understanding of the use of PSA/PRA information to support operating plants:

   -- principles, approaches and methods for the improvement of technical specifications (LCOs, AOTs, STIs);

   -- approaches to the feedback of operational experience to review parameters, assumptions, results and methods of former probabilistic safety assessments;

   -- principles and approaches to optimise plant reliability and maintain plant safety during plants' lifecycles.

3. Development of guidelines to increase applicability of PSA/PRA methods and results:

   -- guidelines for analysts to make PSA/PRA information more applicable to potential users;

   -- common technical understanding of the importance of the limitations and weaknesses of probabilistic methods for the application in decision making processes of:

      -- common mode failures
      -- human failures
      -- uncertainties and completeness
      -- conservative or best estimate assumptions.

REFERENCES

1. NUREG-75/014, "Reactor Safety Study, WASH-1400, October 1975

2. Lewis Report

3. DRS, Deutsche Risikostudie Kernkraftwerke, "Eine Untersuchung zu dem durch Störfälle in Kernkraftwerken verursachten Risiko,: Der Bundesminister für Forschung and Technologie. Verlag TÜV-Rheinland, 1979

4. Rogovin Report

5. Report of the President's Commission on "The Accident at Three Mile Island"

6. NUREG-0880

7. EG Status Report

8. Safety Goals

9. IAEA-TECDOC 308 -- Reliability Analysis and Probabilistic Assessment in the Licensing of Nuclear Power Plants

10. NUREG-1050 Probabilistic Risk Assessment (PRA) Reference Document

11. IREP (Procedures Guide)

12. NUREG-CR 2300, PRA Procedures Guide, January 1983

APPENDIX

Comprehensive survey of examples of PSA/PRA applications in Member countries.

Member State		Contact Person	Decision-making Body	Area of Decision making 1. Generic Regulation 2. Generic R+D 3. Plant-Specific 1.	2.	3.	Title of Application
Australia	1	E.R.Corran	A.A.E.C			X	HIFAR-Safety Analysis Task
	2	E.R.Corran	A.A.E.C			X	Reliability Study of the HIFAR Emergency Core Cooling System
	3	E.R.Corran	A.A.E.C			X	Reliability Analysis of the HIFAR Containment Isolation System
Belgium	1	M.Preat	Licensing Experts			X	Electrical Systems of Doel 1 & 2 NPP
	2	M.Preat	Licensing Experts			X	Auxiliary Boilers Explosions at Doel 1 & 2 NPP
	3	M.Preat	Licensing Body			X	Safety Analysis for Doel 3 & 4 NPP
Canada	1	F.K.King	Ontario Hydro			X	The Darlington probabilistic safety evaluation
Finland	1		V T T			X	Reliability Analysis of safety functions of Loviisa
	2		V T T			X	Reliability Analysis of safety functions of Olkiluoto
	3		V T T			X	Analysis of accident sequences of Secure
France	1	J.M.Lanore	S.C.S.I.N.	X			900 MW-PWR-Risk reduction by adjunction of a gas turbine
	2	J.M.Lanore	EDF-			X	Probabilistic Analysis of Fessenheim power plant systems safety
	3	J.M.Lanore	EDF-CEA/IPSN		X		Probabilistic Studies of system safety in Paluel power plant
	4	J.M.Lanore	EDF-CEA/IPSN	X			Probabilistic Analysis of the loss of redundant safety systems
	5	J.M.Lanore	NERSA-EDF	X	X		Computation of settimes for pieces of egnipment important for safety of Creys Malville power plant using probabilistic methods

Member State		Contact Person	Decision-making Body	Area of Decision making 1. Generic Regulation 2. Generic R+D 3. Plant-Specific 1.	2.	3.	Title of Application
Germany	1	H. Fabian	KWU			X	Improvement of SG-feeding (PWR)
	2	H. Fabian	KWU			X	Reliability of closing of the BWR-Isolation Valves
	3	H. Fabian	KWU-			X	Optimization of plant operation at a SG tube leakage
	4	H. Fabian	KWU			X	Preliminary PRA for the PHWR-plant Atucha II
	5	Kleppmann	TÜV-Stuttgart			X	Coarse-meshed PRA for GKN 2 Power Plant
	6	W. Wachholz	HRB			X	Design Stage Application: High Temperature Reactor
	7	H.-P.Balfanz	TÜV-Nordd.			X	PSA of safety systems of KBR power plant
	8	H.-P.Balfanz	TÜV-Nordd.			X	PSA of reactor protection system of KWG, KKP-2, KBR power plants
	9	H.-P.Balfanz	TÜV-Nordd.			X	PSA of safety systems of KKK power plant
	10	M.Herttrich	-			X	Optimizations as Consequences of the German Risk Study
	11	M.Herttrich	RSK	X			Application of Single Failure Criterion and External Events
	12	M.Herttrich	KTA	X			Classification of Event Sequences for Design Purpose
	13	M.Herttrich	BMI	X			NPP-Safety Criteria/ Probabilistic Approach

Member State		Contact Person	Decision-making Body	Area of Decision making 1. Generic Regulation 2. Generic R+D 3. Plant-Specific 1.	2.	3.	Title of Application
Italy	1	S.Toccafondi	ENEL OR AN-SALDO	X		X	Alto Lazio safety reliability analysis (ALSRA)
	2	G.Russino	ENEL OR NIRA	X		X	PUN PSA Study
	3	A.Valeri	ENEA/DISP	X			Review of ALSRA
	4	A.Valeri	ENEA/DISP	X			Review of the PUN PSA Study perfomed by ENEL/NIRA/W.
	5	A.Valeri	ENEA		X		Core rescue system (SSN) for LWR's
Japan	1	T.Tobioka	Nuclear Safety Commission	X			Licensing Decision on BWR, PWR, LMFBR Safety Systems Design
Netherlands	1+2	H.J. van Grol	Kernfysische Dienst			X	Calculation based on Rasm.-Report for KCD and KCB
Spain	1	J.I.Villadoniga	Plant owner			X	Reliability analysis of the auxiliary feedwater system (AFWS) - ALMARAZ NPP
	2	J.I.Villadoniga	Regulatory Body (CSN)			X	Reliability analysis of the auxiliary feedwater system (AFWS) - ASCO NPP
	3	J.I.Villadoniga	Regulatory Body (CSN)			X	PSA of Santa Maria de Garona NPP
Sweden	1	T.Lilja	Swedish State Power Board			X	Discovery and rectification of a potential common cause failure
	2	T.Lilja	Swedish State Power Board			X	Discovery and rectification of deficiency in system for level indication in RPV
	3	L.Carlsson	Licensing Authority	X			Evaluation of technical specifications and surveillance requirements
	4		Utility and Licensing Authority			X	PRA of Ringhals 1
	5		Utility and Licensing Authority			X	PRA of Ringhals 2

Member State		Contact Person	Decision-making Body	Area of Decision making 1. Generic Regulation 2. Generic R+D 3. Plant-Specific 1.	2.	3.	Title of Application
Switzerland	1	S.Chakraborty	Licensing Authority	X			Reference Core Melt Accidents
	2		Utility and Licensing Authority			X	PRA of Leibstadt
	3					X	PRA of Beznau
United Kingdom	1	F.R.Allen	UKAEA	X			Fuel Pin Ballooning Risk Assessment
	2		CEGB	X		X	PRA of Sizwell
U.S.A.	1	F. Rowsome	US-NRC	X			Prioritization of Safety Issues
	2	F. Rowsome	US-NRC	X			Systematic Evaluation Program (SEP)
	3	F. Rowsome	US-NRC			X	Indian Point ASLB Proceedings
	4	F. Rowsome	US-NRC	X			Pressurized Thermal Shock
	5	F. Rowsome	Common wealth Edison Comp.			X	Indian Point Equipment and Procedural Changes
	6	F. Rowsome	US-NRC	X			Emergency Planning and Response
	7	F. Rowsome	US-NRC	X			Anticipated Transients Without Scram (ATWS)
	8	F. Rowsome	US-NRC	X			Auxiliary Feedwater System Availability
	9	F. Rowsome	US-NRC	X			Value/Impact Assessments for Generic Requirements
	10	F. Rowsome	US-NRC	X			Evaluation of Exemptions from LCO Tech. Specs and Surveillance Reqs.
	11	F. Rowsome	US-NRC	X			Accident Management
	12	F. Rowsome	US-NRC	X	X		NRC Policy on Future Reactor Design

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
Aus 1	Dido 1984 10 MW	Analysis of consequences of - loss of coolant accidents LOCA - reactivity accidents - transport and storage accidents - loss of coolant flow accident	- LOCA is the most significant accident - several ways to reduce hazards - frequency of all accidents $\leq 10^{-5}$	\$ 100 000 8 - 10	6 (3)
Aus 2	- " -	PSA: emergency core cooling system random mode failure examined, no CM-failure because no data	no alternatives of project were necessary	\$ 50 000 1	1
Aus 3	- " -	PSA: containment isolation system - further see Aus 2 -	- test frequencies changed - CMF identified	\$ 50 000 1	1
Bel 1	DOEL 1+2 PWR/W	Electrical power supply and distribution system	Reliability level was adequate	1	1
Bel 2	1975 2x400 MW	Explosion of auxiliary boilers could impair electric power supplies - the onsite power supply diesels (APS)	Addition of redundant protection and control systems, alarms, maintenance and test procedure improvements. Loss of APS $\leq 10^{-7}$	3/4	1
Bel 3	DOEL 3 Tihange 2 PWR/FA 1982 900 MW	Man made external hazards, aircraft crash or explosions (industrial-transportations) Beznau-Typ Aircraft impact Curve/ German Gas-Cloud overpressure Curve	No changes of design necessary, checking against 10^{-7}/y	2	1

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
Can 1	Darling-ton PHWR 1987-1991 4x850 MW	PSA of safety design analyzed to system reliability, system inter-connections, and support system (event tree/fault tree analysis) human reliability forces the analyst to be much more systematic	- ensure adequacy of safety design - provide information base to write abnormal incident operating procedures - assess economic risk - provide supporting material to licens. procedure	$ 3 500 000 (Can) 40	
Fin 1	Loviisa PWR 1977 2x440 MW	Reliability of main safety functions using DBA assumptions with regard to success criteria. Containment and release analysis was done for large LOCA. After few years operation some reanalysis has been done using reliability data based on operating experiences. The new results did agree moderately well with the first estimates.	The analysis led to small modification in the design of safety systems.		
Fin 2	Olkiluoto 1-2 1979 2x660 MW	Reliability of main safety functions using DBA success criteria. Assessment of test and repair arrangements. In a second stage a new analysis has been done for optimization test and repair arrangements and limiting conditions operation.	Verification of the overall reliability of safety systems.		

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
Fin 3	Secure 1978 200 MW/th	Careful identification of potential accident sequences, comparison of design alternatives, containment and offsite consequences analysis for three selected accidents only. Developed models to account time-dependence in accident sequences in respect to long time allowed by reactor pool heat up.	Analysis used as aid to design concept alternatives		
Fra 1	PWR/FA Stand.plant 900 MW	PSA of the loss of electrical supplies. Assessment of risk reduction by adjunction of a gas turbine. AOT for external supply, diesel generators, gas turbine and buses	•Decisions related to operation of equipments •risk increase in case of partial unavailability $\leq 10^{-7}$/event •probability of unaccebtable consequences $\leq 10^{-7}$/a/family of events	FF 500 000 1	2
Fra 2	Fessenheim PWR/FA 1977 900 MW	Assessment of the reliability/ availability of main mechanical, electrical and thermohyd. systems, used fault tree analysis and others. Human factors were considered by Dr. Swain's THERP-method.	Identification of potential weak points: - handling crane, travel spent fuel cask in a low position - steam line isolation valves, modification of periodic tests. - CMF: frost pipes - CVCS: Wrong layout of pipes	8	1

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
Fra 3	Paluel PWR/FA 1984 1300 MW	PSA of main safety systems used FMEA, Fault trees, Markov's diagrams, improved computer codes for FTA, studies were modified incorporating CMF systematically.	Design of safety systems is considered satisfactory and optimized, research effort remained to be made to estimate CMF realistically.	13	1
Fra 4	PWR/FA 1990 1400 MW	PSA of the loss of redundant safety Systems: H_1: loss of heat sink H_2: total loss of feedwater to steam generator H_3: loss of electric power supplies H_4: long term mutual backing of LPSI and CSS pumps in the event of LOCA. Data compiled from 900 MW power plants. Detailed analysis of human factors impact was made, improvements of HF by modifying organisation of control rooms and using computers. All nuclear unit operating conditions were analyzed from power operation up to refueling phase.	PSA indicated only minor changes: H_1: use of CVCS after 8 houres to be able to use charging pump/test H_2: SG are refilled only one by one to avoid rupture of SG-tube if refilling too sudden H_3: test pump suction line will be directly connected RWS-tank instead of CVCS-tank. Unacceptable consequences for each family H_1-H_4 $\leq 10^{-7}$/a	9	2

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
Fra 5	Creys-Malville FBR 1986 1200 MW	PSA: to obtain set-times to be used in the event of unavailability of a number of safety systems. The accident sequence are considered unacceptable if the sodium temperature exceed 650 °C in the primary and secondary circuits.	risk increase in case of partial unavailability $\leq 10^{-7}$	12	3
Ger 1	PWR/ KWU 1985 1300 MW	PSA of SG-feeding systems (secondary side heat removal system) to ascertain that the safety concept is well balanced. The reliability of the secondary side heat removal should be in the same range as other functions, e.g. heat removal via primary side	Improvements by means of a redundant design of the feeding control on the start-up and shut down system, improvements of reliability by a factor of 3-5	low effort	1
Ger 2	BWR/ KWU 1984 1300 MW	PSA of steamline isolation valves under certain loads related to selected accidents, to avoid the excess of unrealistic demands based on formal application of deterministic assumptions.	Comparison of the reliability of the isolation function with the reliability of other safety functions	low effort	1
Ger 3	PWR/ KWU 1985 1300 MW	PSA of plant operation after SG-tube leackage, reactor shut down and emergency power mode can be delayed until return of external grid, leaving the reactor in a hot stand-by condition.	Optimization of plant operation after SG-tube leakage by means of PSA. Deterministic procedure for plant design does not distinguish between likely and unlikely accidents.	low effort	2

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
Ger 4	Atucha II PHWR KWU 1988 740 MW	Preliminary PRA of plant and system design to get the construction permit.	PRA to demonstrate that Argentina risk-criteria are fulfilled, - design is well balanced - safety level comparable to German PWR.	medium	6
Ger 5	GKN-2 PWR/KWU 1988 1300 MW	PSA based on methods of German Risk Study to quantify essential improvements that had been realized in the meantime. Event sequence analyses up to core melt accident and containment failure modes are assessed.	Changes in test strategies and proposals for improvements (e.g. additional energy supply of emergency feed water pumps.) Criteria used: (these are not binding) 1. Is the overall risk dominated by one accident sequence? 2. Is the overall risk dominated by one system? 3. Are the individual contributions to the risk smaller than those evaluated in the German Risk Study for Biblis-NPP?	≤ 1	5
Ger 6	HTR-concept HRB 500 MW	Optimization of safety concept, with regard to - system decay heat removal - liner cooling system for heat removal - filtered vented containment.	Development of a well balanced safety concept. Accident frequences $\geq 10^{-5}$/a (design range) below limit value of 5 rem.		

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
Ger 7	KBR PWR/KWU 1986 1365 MW	PSA of safety system of - emergency core cooling system - heat removal system on the secondary side as SG-feeding system and steam dump station - containment isolation system (CIS) - electrical power supply in respect of the demand of an accident: - large, medium, small LOCA - emergency power case - external events - pipe break on secondary side - steam generator tube break.	Assessment whether the safety concept is well balanced. Identification of special important safety features - CIS of pump seal-cooling system by the chance of a break following a LOCA - asymmetric steam dump on secondary side influencing natural ciculating on primary side by a small LOCA - isolation of accumulator after water discharge to prevent pressure gas discharge by a small LOCA - feeding control on start-up and shut down system (s. Ger 1)	1	2
Ger 8	KWG KKP-2 KBR PWR/KWU 1985/ 1986 1361 MW	Similar reliability analyses of reactor protection systems (RPS) because of identical system layouts of the three PWR's. - Detailed fault tree analysis of the most complex channel - simplified analysis of all other channels - detailed failure rate predictions of new electronic devices (ED) - judgment of assessed unavailability of channels due to the influence of results in the PSA described under Ger 7.	- Necessity to distinguish the failure mode of ED to revealed and unrevealed failure - improvments of monitoring devices - some reductions of test intervalls	2	2

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
Ger 9	KKK BWR/KWU 1984 1316 MW	PSA of safety system of - emergency core cooling system - containment isolation system - scram-system - reactor protection system - electrical power supply - turbine protection system - fuel element storage pool cooling system analyzed due to the demand of selected and representative accidents.	Assessment whether the safety concept is well balanced. - Determination of test intervals and allowed outage times - installation of additional check valves to prevent excessive flooding of reactor building by a break of a cooling water-line. - extensive surveillance test-procedures of safety and depressurization valves to prevent common mode failures.	2-3	1/2
Ger 10	Biblis B PWR/KWU 1976 1300 MW	Optimizations as consequences of the German Risk Study-Phase A: Technical improvements were carried out in NPP-Biblis B and in other similar PWR e.g. to relieve the operator in a course of an accident.	Some special results: - Position indication (limit switch) at the pressurizer relief valve - Interlock of relief isolating valve (automatic start at $p < 125$ bar <u>and</u> $T > 280$ °C) Availability of the secondary system (in case of small LOCA): - semi-automatic shut-down with 100 °/h - control of the shut-down of the secondary system (better presentation of measurements) - water level measuring of the steam generator to withstand greatest anticipated accident		

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
Ger 11	BWR	Application of single failure criterion to external events: The emergency steamline outside containment and the electrical power supply of the second isolation valve were not designed to withstand the safety earthquake (SE). The frequency (F) of the sequence up to an unisolated LOCA was assessed.	Frequency of SE $< 10^{-5}$/y Valve failure to close 1.10^{-2}/demand F (LOCA) $\bar{}$ 10^{-7}/y. Because of this rare event no redundancy was necessary.		
Ger 12	General application	Classification of event sequences for design purposes: About 80 different initiating events and event sequences as transients and LOCA's based on the experience with the design, licensing and NPP operations of German PWR and BWR were estimated. These events are ranked by their frequency and divided in five classes for the purpose of design objectives: The more frequent the class the greater the safety margin. (KTA-GS-47, Klassifizierung von Ereignisabläufen, June 1985)	Class of events:		
			1 Normal operation	few mrem/year maximum allowable level: 30 mrem/y	
			2 Transients, abnormal occurences $>3.10^{-2}$		
			3 Improbable accidents $3.10^{-2} - 10^{-4}$	below 5 rem/event	
			4 design basis accidents (hypothetical) $10^{-4} - 10^{-5}$		
			5 Beyond design base $< 10^{-5}$	over 5 rem	

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
Ger 13	General application	The most important probabilistic requirement in the FRG is contained in the BMI*-Nuclear Power Plant Safety Criteria. In criterion 1.1: "Basic principles of Safety Precautions" the defence in depth concept is laid down and it is specified:		Probabilistic Approaches	
		1. According to common engineering experience, malfunctions of plant components or systems (abnormal operating conditions) can occur during the lifetime of the plant. To control these abnormal operating conditions, systems shall be provided for operational control and monitoring. These systems shall be designed such that incidents as a result of abnormal operating conditions are avoided with a sufficient reliability*)			
		2. Beyond the above as a second principle, measures shall be taken to control incidents. For this, sufficiently reliable*) engineered safeguards shall be provided. These engineered safeguards shall be designed such that the personnel and population is guarded against the effects of incidents.		Probabilistic acceptability criteria	
		*) Comment regarding methodology:		Relative probabilistic criteria	
		To ascertain that the safety concept is well balanced, the reliability of systems and plant components important to safety - supplementing the overall assessment of the nuclear power plant's safety on the basis of deterministic methods - shall be determined with the aid of probabilistic methods as far as the required accuracy can be achieved according to the state of science and technology.		Probabilistic analysis of important systems Probabilistic methods supplement deterministic Scope and depth of probabilistic according the state of the art	

* BMI = Federal Ministry of the Interior

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
Ita 1	Alto Lazio BWR/GE 1987 2x1000 MW	PSA to evalute the reliability of transient and accident mitigation systems by assessment of frequency of events, which result in exceeding licensing criteria, as - core cooling failure - containment failure - licensing dose limits. All parties involved in PSA gained a better understanding of BWR response to anticipated initiating events.	280 design change recommendations were made.	$ 2 Mill. 16	3
Ita 2	PWR NIRA/W 1991 2x1000 MW	PSA to a systematic assessment of plant behaviour accident conditions. Experience was gained in the field - balanced assessment of plant defences; - importance of support and front line systems; - human factors; - common mode failures; - development of methodologies for alternatives comparison.	Various design modifications based on PSA. Reference values of core damage probability, $10^{-6} - 10^{-7}$/a for each individual sequence, $10^{-5} - 10^{-6}$ for all sequences.	$ 3 Mill. 15	4
Ita 3	s. Ita 1	Review of PSA of Ita 1 performed by ENEL/ANSALDO GE. The review will assess compliance of ALSRA with requirement attached to contraction permit of the plant concerning the adequacy of the reliability levels of its protective functions.			3

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
Ita 4	PWR NIRA 1000 MW	Review of the PUN probabilistic safety study performed by ENEL/NIRA/W. The review will assess compliance of PUN with general safety criteria for the Italian Standard Plant which include the application of the PSS with use of numerical targets related to probability of accidents leading to degraded core conditions.		$ 170 000	4
Ita 5	PWR W/B&W 788 MW (for future PWR in the next 10 years)	Evaluation of the core melt frequency reduction of a core rescue system on a reference plant. The reference plant is a 3 loop W312 or Surry 1 respectively. Dominant core melt sequences were derived form the PRA Studies: 1. Surry (WASH-1400) 2. Zion (Comm. Edison) 3. Sequojah (RSSMAP) 4. Indian Point 2 (Consolidated Edison) 5. Indian Point 3 (PASMY) 6. Sizewell B (CEG B) Extensive use was made of RSS (WASH 1400) and utilities risk studies conducted on plants similar to the Italian PUN.	Target: Core melt frequency reduction by a factor of at least 10 by means of a passive type system called Core Rescue System (SSN).	1/2	4

Member State	Type year power	Description of Analysis			Results/ Criteria	Cost person years	Level of PSA
Jap.	TEPCO BWR/MkII	PRA Level 3	1980	Fukushima	Off-site dose criteria:		
	KEPCO PWR/W 3 Loop	PRA Level 3	1980	Mihama			
	JAPCO BWR 2	PRA Level 3	1985	Tsuruga			
	PWR/W 3 Loop	PRA Level 3	1986	Takahama			
	FBR	PRA Level 4	1980	Monjyn			
Neth 1	Dodewaard BWR/GE 1968 52 MW	The purpose of the study was to make a complete risk analysis of all the aspects of the fuel cycle occurring in the Netherlands. A complete PRA was only made for the Borssele station, a PWR of KWU design (KCB) and the Dodewaard station, a BWR of GE design. For a 1000 MWe PWR or BWR for five different sites in the Netherlands PRA's were performed on the levels 5 up to 8.				5	8
Neth 2	Borssele PWR/KWU 1973 450 MW					10	8

Off-site dose criteria:

	Frequency	Whole Body	Thyroid
- Anticipated operational occurence	$>10^{-2}$	5 mrem/y	15 mrem/y
- Accident	10^{-2}./.10^{-4}	500 mrem	1,5 rem
- side evaluation accident	$>10^{-6}$	25 rem	150 rem* 300 rem **
- events not considered	$<10^{-6}$		

* for infant
** for adult

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
Spa 1	Almaraz PWR 930 MW	PSA of the auxiliary feedwater system (AFWS), to decide if some modifications were necessary. Major steps of analysis: a) Documents collection. b) Development of fault-trees for the following initiating events: - Loss of main feedwater. - Loss of main feedwater due to a loss of off-site electrical power. - Loss of main feedwater together with total loss of a.c. power. c) Quantification of the system reliability from data of component failures, human errors, test and maintenance. d) Common mode failures analysis. e) Uncertainties analysis. f) Results interpretation.	Changes in calibration procedures to avoid common mode miscalibration of certain redundant sensors. Changes in test procedures to double check alignment of a valve in the steam driven pump train. Change in administrative procedures to treat this valve as locked open. A better knowledge by the plant operator of the strengths and weaknesses of the system.		1
Spa 2	ASCO	PSA of AFWS fails to perform its safety function on demand and to decide if some modifications are necessary.			1

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
Spa 3	St. Maria de Garona BWR/GE Mark I 460 MW	The PRA will comprise the assessment of core melt frequencies and their dominant contributors. External events are not included.	The analysis is aimed at: a) The determination of the most significant contributors to the "risk" of the plant. b) The discussion of the back-fitting actions that would be required by the licensing review underway, review that is performed comparing the plant characteristics with current regulatory criteria. c) The introducing and spreading of the PRA techniques in Spain.		4
Swe 1	Ringhals 1 BWR/AA 1974 750 MW	The PSA study was done as part of a general program for recurrent safety analysis of Swedish nuclear plants.	Discovery and rectification of a potential common cause failure: The PSA revealed that some protection systems were connected to the same overcurrent protection switch as non-safety equipment inside containment, that was not qualified for accident environment. An accident causing short-circuit in the non-safety equipment might put some safety systems out of action. The deficiencies have been rectified.		4

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
Swe 2	Ringhals 1	See Swe 1 The problem area was revealed as a result of the systematic and detailed analysis of system functions that the part of PSA studies. Although the same result might in principle have followed from an analysis emphasizing deterministic criteria, our experience suggests that comprehensive and thorough PSA analysis is a valuable check of traditional safety assessments.	In the course of a PSA study it was found that the design of the power supply to the water level indicators in RPV was deficient since two out of three detectors were fed from the same bus-bar. The system had therefore lower reliability than expected, and the PSA study revealed that the impact of this system defect on the total safety of the plant was not insignificant. The defect was corrected at the earliest opportunity.		
Swe 3		Evaluation of technical specifications and surveillance requirements: The Inspectorate has used probabilistic studies of quite varying depth and scope to get bases for decisions as the limiting conditions for operations (LCO) and for temporary exemptions from such conditions.	As a far comparisons have been made with reference figures for reliability etc., such figures habe been considered to have a quite informal character. An element of judgement is believed to be important in decisions on LCO:s.		

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
Swe 4	Ringhals 1 DWR/AA 1974 750 MW	Scope of the PRAs completed: Fires, rare external events and containment behaviour have not been considered. Common cause failures have been considered.	Probability of Core Melt: Mean 2.4×10^{-5}/y		
Swe 5	Ringhals 2 PWR/W 860 MW	See Swe 4	Probability of Core Melt: Median 3.6×10^{-6}/y Mean 5.2×10^{-6}/y		
Swi 1	Goesgen PWR/KWU 1984 970 MW	Selection of reference accidents for preplanning of emergency measures in the environment of a NPP to mitigate the consequences of severe accidents. The accident spectrum was chosen by reference accidents which covers an occurence probability, beyond the range of the design basis accidents, up to about 10^{-6} per reactor-year. The areas of emergency planning were calculated deterministically according to the atmospheric dispersion for some typical weather conditions. The PRA includes analyses of containment failure, off-site consequences and common cause failures. External events and fires are considered only from the point of view of the probability of initiating events.	- Categorize the full spectrum of core-melt accident sequences as 2 types of accidents: early release and delayed release of radioactive materials. - Determination of relative probabilities of these two types of accidents. - Select one which covers most of the total core-melt frequency Probability of CM: 5.6×10^{-6}/y (Mean value)	Sfr 500 000 10	6

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
Swi 1		<u>Comments:</u> Through the exercise of conducting a plant specific PRA-Study one gains engineering judgement for a reasonable definition of reference core-melt accidents for emergency planning. As a by-product the approach enables a straightforward comparison with respect to the effect of design differences between the reference plants. During the plant specific PRA's some weak points in the safety concept of the considered plants have been identified. A review of the proper balance of the safety concepts of nuclear installations obtained by deterministic design principles is possible. The result of such kinds of PRA-Study are only approximate because some simplications and engineering judgement are always necessary. It is not the precision of the absolute numbers which is required but rather the correct relative trends.			
Swi 2	Leibstadt BWR/MkII GE 1000 MW	PRA includes analysis of containment failure, off-site consequences. No detailed common-mode analysis is included. External events such as fire, flood, earthquakes or airplane crash are not considered.	Probability CM: 4.2×10^{-6}/y		

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
Swi 3	Beznau I, II PWR/W 2x350 MW	The PRA will comprise the assessment of core melt frequencies and the analysis will also include consideration of common cause failures by the following external events: Seismic events, fires, flooding, sabotage actions, airplane crash, others (lightning, extreme wind).	- Emergency planning, - developing accident management - further discussion of the rationale and the scope of the back-fitting program of the plant.	15	
UK 1	PTR SGHWR/ UKAEA 1968 100 MW	Fuel Pin Ballooning Risk Assessment: To determine if the original fuel developed for SGHWR - and operated for many years - was adequate to cope with a developing perception of fuel pin ballooning under accident conditions and its effect on emergency spray cooling performance. - Identification of the problem - LOCASTAG - Development of a fuel pin ballooning assessment criteria based on out-of-pile experimental data which were generated. - Development of a fuel pin ballooning risk assessment methodology. - Application to the existing fuel element design and the development of new designs.	Criteria used: - Farmer criterion for a prototype reactor. - "5 % in 300 sec" fuel pin ballooning criterion. Both are formal and binding. Successful development of new 60 pin and 57 pin fuel elements to reduce the integrated risk of losing emergency spray cooling effectiveness under severe loss-of-coolant accidents with flow stagnation (LOCASTAG). All SGHWR fuel elements are now 60 pin and 57 pin designs.		6

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
UK 2	Sizewell B PWR/W 4 Loop 1110 MW	PRA (Westinghouse study) covers the primary circuit thermal-hydraulic analysis and the response of the containment. It includes an analysis of common-cause failures. Offsite consequences are assessed in the NRPB study. External events such as fires, floods, missiles and seismic events have not been addressed in the initial assessments.	Total Degraded Core Frequency: 1.16×10^{-6} per r.o.y.		3

The CEGB's three fundamental reliability criteria are formally expressed as follows:

1. For any single accident which could give rise to a large uncontrolled release of radioactivity to the environment resulting from some or all of the protective systems and barriers being breached or failed, the frequency of occurrence should be less than 10^{-7} per reactor year.

2. The total frequency of all accidents leading to uncontrolled releases should be less than 10^{-6} per reactor year.

3. The predicted frequency of accidents from which radiation doses equivalent to 1 ERL (eg 10 rem whole body dose) could be expected, should not exceed 10^{-4} per reactor year.

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
US 1	General appli-cation	Resource Allocation for Generic Issue Resolution Prioritization of Safety Issues - During the past several years the USNRC has identified nearly 400 issues that could affect the safety of nuclear power plants. To focus regulatory attention on the most important issues, a method was developed to prioritize these issues. This method uses information on the risk reduction potential of the issue and the cost to the utility and the NRC of implementing changes to respond to the issue to designate issues as high, medium or low importance. NRC resources are focused on resolving issues of high importance. Medium priority issues are addressed if resources are available. Low issues are not considered unless new information surfaces that could change their importance to reactor safety. Extensive use was made of existing plant specific analyses such as RSSMAP, IREP, and utility risk sutdies. PSAs are modified to show the effect of each issue before and after hypothetical issue resolution, in order to estimate the person-rem per unit year averted by issue resolution. The results of this effort were published in NUREG-0933. Probabilistic analysis has become an integral part of NRC procedures for evaluating new reactor safety issues. The NRC is also using the issue prioritization work as a management tool for allocating staff resources and money for contractor support.		Typical $ 10000 per issue .04	8

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
US 2	General appli-cation	Systematic Evaluation Programm (SEP) - To support the integrated assessment phase of the Systematic Evaluation Program (SEP), analyses were performed to determine the risk significance of selected SEP topics. Proposed modifications that would upgrade the plant to current licensing criteria were evaluated to determine their effect on core-melt frequency and risk. The results were considered in arriving at backfit decisions. Many issues, such as loose-parts monitoring and RCS leak detection, were found to have low risk importance for virtually all the plants reviewed. Other issues were often found to have high risk importance. These studies have provided useful insights and allowed resources to be applied to the areas where the greatest reduction in risk could be achieved. This experience has shown that even limited PSA/PRA results can provide important information in the regulatory process. The cases in which a plant specific PRA were available worked much better than cases in which importance-to-risk judgements had to be inferred from surrogate PRA's. It appears that severe accident vulnerabilities discovered by the plant specific PRA (where available) were more important to safety, in general, than the instances of non compliance with today's requirements.			

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
US 3	Indian Point 2+3 PWR / W 1974,1976 873 MW 965 MW	<u>Indian Point Probabilistic Safety Study:</u> As a result of the accident at Three Mile Island the NRC recognized the need to reexamine the capabilities of nuclear power plant to accommodate the effects of degraded-core and core-melt accidents beyond the present "design basis accident". Based on a series of intermediate studies and the filing of a petition by a public interest group, hearings were initiated on whether Indian Point should be shut down or other regulatory action taken. The NRC deferred their decision regarding these two units until completion of the formal risk assesment and ASLB hearings. The Commission has yet to rule, although the ASLB has issued its findings and recommendations. The ASLB concluded and recommended to the NRC Commissioners that the facility be allowed to continue operation. A loose parts monitoring system and safety assurance program were recommended. The utility implemented a number of specific modifications on a voluntary basis that were indicated by the safety studies. Inclusion of PRA results in formal hearings established a procedence for considering PRA results in operational decisions.		$ 6,000,000 100 NRC Staff Review: $ 600,000 NRC Staff Review: 10	8

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
US 4	General appli-cation	Pressurized Thermal Shock Renewed interest in pressure vessel failure resulted from the observation that transients could occur in pressurized water reactors characterized by severe overcooling, causing thermal shock, concurrent with or followed by repressurization. The observed transients are subjecting pressure vessels to unanticipated loadings which could contribute significantly to the failure probability. Probabilistic assessments were made of the low frequency failure events and the vessel fracture propagation phenomena. In addition, various utilities performed analyses of the low frequency failure events. Reactor Vessel Pressure Transient Protection for Pressurized Water Reactors, NUREG-0224, September 1978			

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
US 5	Indian Point 2 PWR / W 1974 873 MW	Indian Point Equipment and Procedure Modifications The Indian plant was chosen as one of the plants to initiate activity (see US 3) because the facilities were judged to contribute a significant fraction of the risk to society from nuclear power plants. This judgment was principally based upon the close proximity of the facility to large population centers and an extrapolation of information from the Reactor Safety Study, WASH-1400. In response to the NRC position the utilities performed a small scale, plant-specific risk assessment study, which concluded that the risk from the Indian Point facility was considerably less than that indicated by WASH-1400. NRC reviewed this study and raised several major technical questions. The utility subsequently decided to perform a formal and extensive PRA. The utility implemented a number of specific modifications on a voluntary basis that were indicated by the safety studies. These modifications were to be low-cost ways of reducing the frequency of dominant accident sequences identified in the PRA. These modifications included: Modification to structures to reduce the potential for an earthquake to disable the control room installation of alternate power lines to several pumps to reduce the potential for a fire to result in reactor-coolant-pump-seal failure, and chance in tech specs to require shutdown during hurricane situations to reduce the chance of loss of all AC power.		\$ 1000000 100	8

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
US 6	General appli-cation	<u>Emergency Planing and Response</u> Prior to the occurence of the Three Mile Island incident, various state and local goverments were expressing concern that they were not receiving adequate guidance from the NRC in the area of emergency planning and response. The NRC fromed a task force. The objective was to reach a consensus regarding which accidents should be considered in the emergency response planning and what were the anticipated consequences of those accidents. Several studies have been performed to provide guidance for emergency planning response. Their results formed the basis for the implementation of emergency planing zones for the plume-exposure pathway and for the NRC staff recommendations regarding the use of thyroid-blocking agents.			
US 7	Typical scram system for each of the four U.S. reactor vendors	<u>Anticipated Transients Without Scram (ATWS)</u> In 1969 the Advisory Commitee on Reactor Safeguards (ACRS) raised the possibility of the simultaneous occurence of a reactor transient and the failure of the reactor trip system to automatically shut down the reactor. This type of event was called an Anticipated Transient Without Scram (ATWS). Over the next ten years, this issue was the subject of continuing series of studies that examined the response of light water reactors to ATWS events, the reliability of the scram system and the availability of alternative methods to shut down the reactor if the scram system did not function as designed. The initial studies were deterministic, but subsequent to the release of WASH-1400, probabilistic methods were applied by both the industry and the NRC staff. The evaluation highlighted the relative frequency of severe ATWS events for various reactor types and estimated the expected reductions in frequency for various postulated plant modifications. The study employed PRA-based benefit analyses of the regulatory options for issue resolution.			1 for RPS extended to 8 for ATWS accident sequence

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
US 8	All operating U.S. PWR s	<u>Auxiliary Feedwater System Availability</u> Studies of the accident at Three Mile Island concluded that the Auxiliary Feedwater System was an important safety system in mitigating the effects of this type of accident. Because of this, the USNRC initiated an investigation of the reliability of AFW systems at all operating PWR's. These studies indicated that there was a variation of a factor of 100 in the reliability of AFW systems designed to the same licensing criteria. The studies found that these variations were primarily caused by dependency of the AFWs on support systems and differences in the suction side valving and means of actuation. These studies identified the need for new regulatory requirements for AFWs reliability. The variation in the reliability of the AFWS at operating plants demonstrated that previous regulatory requirements were not adequate. The results of the reliability studies enabled the NRC to develop deterministic regulatory requirements to preclude the types of interactions and failures that were found in the studies to significantly degrade the performance of the AFWS. A numerical goal for AFWS reliability was also adopted as part of the Standard Review Plan. This has resulted in an AFWS reliability study being perfomed for all new plants as part of the licensing process. These studies use the same methods and data as the studies perfomed for operating to develop the information needed for the regulatory action.		30.000 1/3	1 supplem. by 4 for relevant accident sequence

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
US 9	General appli-cation	Value/Impact Assessments for Generic Requirements (CRGR) - In January 1983, the U.S. Nuclear Regulatory Commission published a set of Regulatory Analysis Guidelines, NUREG/CR-0058, for application on all proposed and final rules submitted for review by the Committee to Review Generic Reqiurements (CRGR) or for decision by the Executive Director for Operations or the Commission. These guidelines established a flexible framework for analyzing alternative regulatory actions and contain instructions and describe information needed to support a regulatory analysis. At a minimum the analysis must include a value/impact assessment. In December 1983, the NRC published a handbook, NUREG/CR-3568, for performing the value/impact assessments. The methods described in this handbook include allowance of PRA methods as part of the value/impact assessment. Decisions regarding the resolution of generic issues such as 'leak before break' and 'waterhammer' have been influenced through the use of PRA's prepared under these guidelines.			
US 10	General appli-cation	Evaluation of Exemptions from LCO, Tech Specs and Surveillance Regs. Probabilistic models have been used by the staff to perform sensitivity studies for providing insights into the bases for limiting conditions for operation (LCO's), LCO extensions, and testing and maintenance requirements. Some specific examples include allowed outage times for auxiliary feedwater systems and diesel-generator LCO extensions.			

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
US 11	General appli-cation	Accident Management: There currently exists a large body of requirements for nuclear power plant Emergency Response Capabilities. These requirements are contained in NUREG-0737-Supplement 1-Requirements For Emergency Response Capability (Generic Letter No. 82-33), and contain the following provisions: * Control Room Design Review; * Development of function oriented emergency operating procedures; * Design of the Safety Parameter Display System (SPDS); * Improved Emergency Response Facilities; * Design of instrument displays; and * Operating staff training. Accident Management is defined to be the integration of these features to develop an enhanced operator ability to comprehend plant conditions and cope with emergencies. In addition to these requirements, the NRC is sponsoring a large research and development program in the Accident Management area. This program would utilize the results of the severe accident research program to better understand the physical conditions that could occur during an accident. Probabilistic Risk Assessment techniques associated with accident sequence progression (e.g., Operator Action Event Trees) are also being developed to provide a comprehensive approach to understanding the development and progression of accident sequences and provide an integrating technique to coordinate the existing emergency response capabilities.			

Member State	Type year power	Description of Analysis	Results/ Criteria	Cost person years	Level of PSA
US 12	General application	NUREG-1070, "NRC Policy on Future Reactor Designs": Decisions on Severe Accident Issues in Nuclear Power plant Regulation In response to insights gained from Probabilistic Risk Assessments and the Accident at Three Mile Island, in 1980 the NRC undertook to develop a policy statement on severe reactor accident issues. NUREG-1070 presents the current NRC position on severe accident issues (NRC Policy Statement). In addition, the document describes related NRC Severe Accident programs such as the Severe Accident Research Program, TMI lessons learned, safety goal evaluation, resolution of Unresolved and Generic Safety Issues, source term revisions and siting policies. Questions concerning treatment of uncertainties in severe accident decision-making; the manner that new safety information will be used in the regulatory process; and a generic regulatory decision strategies are also discussed. Finally the document encourages the use of Systems Reliability Assurance Programs, by the industry to provide a continuing level of safety analysis used in the licensing and regulatory process. Within the Commission Policy Statement, the Commission concludes that "existing plants pose no undue risk to public safety and property and sees no present basis for prompt action on generic rulemaking or other regulatory changes for these plants because of severe accident risk". Further, the Commission finds that a new design for a nuclear power plant can be acceptable if it meets the following criteria: * Compliance with current regulations 10 CFR 50; * Resolution of applicable Unresolved Safety Issues and Generic Safety Issues; * Completion of a Probabilistic Risk Assessment with due consideration to severe accident vulnerabilities; and * Acceptance of design by staff in safety review.			