SAFETY SERIES No. 75-INSAG-6

SAFETY REPORTS

safety series

INSAG-6
Probabilistic Safety Assessment

A REPORT BY THE
INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP

INTERNATIONAL ATOMIC ENERGY AGENCY, VIENNA, 1992

CATEGORIES IN THE IAEA SAFETY SERIES

A new hierarchical categorization scheme has been introduced, according to which the publications in the IAEA Safety Series are grouped as follows:

Safety Fundamentals (silver cover)

Basic objectives, concepts and principles to ensure safety.

Safety Standards (red cover)

Basic requirements which must be satisfied to ensure safety for particular activities or application areas.

Safety Guides (green cover)

Recommendations, on the basis of international experience, relating to the fulfilment of basic requirements.

Safety Practices (blue cover)

Practical examples and detailed methods which can be used for the application of Safety Standards or Safety Guides.

Safety Fundamentals and Safety Standards are issued with the approval of the IAEA Board of Governors; Safety Guides and Safety Practices are issued under the authority of the Director General of the IAEA.

An additional category, **Safety Reports** (purple cover), comprises independent reports of expert groups on safety matters, including the development of new principles, advanced concepts and major issues and events. These reports are issued under the authority of the Director General of the IAEA.

There are other publications of the IAEA which also contain information important to safety, in particular in the Proceedings Series (papers presented at symposia and conferences), the Technical Reports Series (emphasis on technological aspects) and the IAEA-TECDOC Series (information usually in a preliminary form).

PROBABILISTIC SAFETY ASSESSMENT
INSAG-6

A report by the International Nuclear Safety Advisory Group

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ARGENTINA
AUSTRALIA
AUSTRIA
BANGLADESH
BELARUS
BELGIUM
BOLIVIA
BRAZIL
BULGARIA
CAMBODIA
CAMEROON
CANADA
CHILE
CHINA
COLOMBIA
COSTA RICA
COTE D'IVOIRE
CUBA
CYPRUS
CZECHOSLOVAKIA
DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA
DENMARK
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ESTONIA
ETHIOPIA
FINLAND
FRANCE
GABON
GERMANY
GHANA
GREECE
GUATEMALA
HAITI
HOLY SEE
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
LEBANON
LIBERIA
LIBYAN ARAB JAMAHIRIYA
LIECHTENSTEIN
LUXEMBOURG
MADAGASCAR
MALAYSIA
MALI
MAURITIUS
MEXICO
MONACO
MONGOLIA
MOROCCO
MYANMAR
NAMIBIA
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
PAKISTAN
PANAMA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
ROMANIA
RUSSIAN FEDERATION
SAUDI ARABIA
SENEGAL
SIERRA LEONE
SINGAPORE
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
THAILAND
TUNISIA
TURKEY
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
VENEZUELA
VIET NAM
YUGOSLAVIA
ZAIRE
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world".

Printed by the IAEA in Austria
July 1992

SAFETY SERIES No. 75-INSAG-6

PROBABILISTIC SAFETY ASSESSMENT

INSAG-6

A report by the
International Nuclear Safety Advisory Group

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 1992

The International Nuclear Safety Advisory Group (INSAG) is an advisory group to the Director General of the International Atomic Energy Agency, whose main functions are:

(1) To provide a forum for the exchange of information on generic nuclear safety issues of international significance;
(2) To identify important current nuclear safety issues and to draw conclusions on the basis of the results of nuclear safety activities within the IAEA and of other information;
(3) To give advice on nuclear safety issues in which an exchange of information and/or additional efforts may be required;
(4) To formulate, where possible, commonly shared safety concepts.

THIS SAFETY SERIES IS ALSO PUBLISHED IN FRENCH, RUSSIAN AND SPANISH

VIC Library Cataloguing in Publication Data

Probabilistic safety assessment : INSAG-6 : a report by the International Nuclear Safety Advisory Group. — Vienna : International Atomic Energy Agency, 1992.
p. ; 24 cm. — (Safety series, ISSN 0074-1892 ; 75-INSAG-6)
STI/PUB/916
ISBN 92-0-102492-4
Includes bibliographical references.

1. Nuclear power plants—Risk assessment. 2. Nuclear reactors—Safety measures. 3. Nuclear power plants—Reliability. I. International Atomic Energy Agency. II. International Nuclear Safety Advisory Group. III. Series.

VICL 92-00022

FOREWORD
by the Director General

Probabilistic safety assessment (PSA) has contributed significantly to the understanding of how best to ensure the safety of nuclear power plants. By means of PSA, a nuclear power plant, including its safety systems and installations, can be analysed in its entirety. Such an analysis can yield insights into plant processes and mechanisms and possible interactions between plant systems, both for existing plants with operating histories and for plants still in the design stage.

The rapid development and increased use of PSA and its methods in recent years have been accompanied by some exaggerated claims of its capabilities and of the applicability of the results of PSA in safety analysis, plant design, and the regulation and control of operating practices. Concern over the misapplication of PSA and its methods and the misinterpretation of the results of PSAs led INSAG to prepare the present report, Probabilistic Safety Assessment, on its merits and limitations.

I am pleased to have received this report and am happy to release it to a wider audience.

CONTENTS

1. INTRODUCTION

At nuclear power plants, extensive safety precautions are aimed at reducing the possibility of accidents with serious consequences. The necessary level of safety is demonstrated and monitored by analysis and by compilation of information on operating experience.

Most safety analyses in the past did not explicitly consider probabilities. Compliance with safety requirements was checked by deterministic analyses that used pessimistic assumptions in order to ensure that the results of assessments were 'on the safe side'.

Operating experience with proven reactor designs shows that events of direct safety relevance have been rendered more and more scarce by the safety precautions that have been taken. However, the lack of events of safety significance in an individual case does not preclude the existence of underlying safety deficiencies. Thus, there is a gap between the bulk of operating experience and events of safety significance which may be bridged only by theoretical analysis.

Probabilistic safety assessment (PSA) is a systematic approach to performing that analysis. Its use is closely related to the use made of operating experience in general.

The rapid development of the method has resulted in its extensive use, possibly at times beyond the point of satisfactory application. This report therefore reviews the general bases of probabilistic safety assessment, emphasizing its merits and limits as well as the general lines of the future development of that methodology and its application.

In this report, some of the discussion of PSA, its methods and its results may seem very negative. If so, this is because of INSAG's conviction that PSA, if properly conducted, is an important tool in achieving safety, and INSAG believes it is essential to highlight the areas where most benefit can come from improvement of the methodology.

2. CAPABILITIES AND LIMITATIONS OF THE METHODOLOGY OF PSA

2.1. HISTORICAL BACKGROUND

The first large scale applications of probabilistic methodology to nuclear safety were the risk analyses performed in the 1970s successively in the United States of America, the United Kingdom, the Federal Republic of Germany and other countries. In particular the analysis in the USA [1] and the German investigation [2, 3] were aimed at the calculation of individual and population risks from the operation of nuclear power plants, and comparison with other natural and industrial risks. Earlier applications of statistical methods, for instance in the aircraft industry, were limited to reliability analyses.

Originally it was believed that these methods could be used for generating probabilistic acceptance criteria for the development of nuclear power. At some stage comparisons with general risks in life, and with goals for risks to individuals and populations, were proposed in the USA and discussed in several other countries. However, the use of quantitative safety goals in regulatory requirements turned out to be difficult. The main reasons were the dependence of the results of PSA on the scope and methodology, and on subjective elements, as well as a lack of plant specific data suitable for obtaining sufficiently accurate results.

On the other hand, the first risk analyses provided important insights into strengths and weaknesses of design and operation of the plants under investigation. For instance, WASH-1400 [1] and the German study [2, 3] demonstrated the significance of small break loss of coolant accidents (LOCAs) for pressurized water reactors (PWRs). The investigations also pointed to possible ways to improve the plants' safety. PSAs have subsequently been carried out for many existing plants and for new designs, and they have continued to confirm the benefit of PSA in identifying plant weaknesses to be remedied. In addition, attempts to develop safety goals and technical acceptance criteria have continued.

The 'state of the art' is described in some detail by the IAEA Safety Series report The Role of Probabilistic Safety Assessment and Probabilistic Safety Criteria in Nuclear Power Plant Safety [4] and by the NUREG-1420 peer review [5] of NUREG-1150 [6].

2.2. GENERAL ASPECTS OF PSA

In practice, PSA aims at:

— identifying and delineating the combinations of events that may lead to a severe accident;

— assessing the expected probability of occurrence for each combination;
— evaluating the consequences.

In order to perform these tasks, PSA methodology integrates information about plant design, operating practices, operating history, component reliability, human behaviour, accident phenomena, and (in its widest application) potential environmental and health effects. The approach aims at achieving completeness in identifying possible mishaps, deficiencies and plant vulnerabilities, and providing a balanced picture of the safety significance of a broad spectrum of issues, including the uncertainties of the numerical results.

Customarily, three levels of PSA are distinguished, depending on the scope of the analysis:

— A Level 1 PSA provides an assessment of plant design and operation, focusing on sequences that could lead to core damage. It can provide major insights into design strengths and weaknesses and into ways of preventing core damage that would be a precursor to a large release of radioactive material.
— In addition to the analyses performed in a Level 1 PSA, a Level 2 PSA also addresses the phenomenon of a core damage accident, the response of the containment to the expected loads, and the transport of radioactive material from the damaged core to the environment. Such analyses provide information about the probabilities of accidental radioactive releases (source terms). The analyses show the relative importance of events in terms of the primary safety concerns arising from the possibility of off-site releases, and they allow the identification of measures for mitigation of the consequences of accidents.
— In addition to the aspects analysed within a Level 2 PSA, a full scope or Level 3 PSA also analyses the dispersion of radionuclides in the surrounding environment and potential environmental and health effects.

At each level, PSA provides the probabilities (frequencies) of adverse consequences and information on the dependence of these values on specific technical features (risk profiles). These findings depend to some degree on subjective elements in the various steps of the analysis.

2.3. SOURCES OF DATA

The general approach to PSA is to define a set of initiators that challenge the safety of the plant and then to derive the probability of sequences of events leading to unacceptable consequences beyond the design basis, using a detailed plant model, initiator probabilities and component reliabilities. Data required relate to reliabilities of components, systems and operator actions. One approach is to use databases that summarize all pertinent data. Some of the data will be from plants with different

operating conditions and from components with different detailed designs (generic data). An alternative and preferable approach is to use information on direct operating experience from the particular plant to estimate initiator probabilities and system failure probabilities (plant specific data). In practice, a combination of the two approaches is used.

2.4. TYPE OF ANALYSIS

Ideally, two types of PSA may be distinguished.

- The first type of analysis, termed a posteriori analysis, refers to existing plants with operating histories. It is based on information from past operating experience, normally plant specific data. For instance, each event identified from historical records may be analysed to determine the conditional probability of its progression to an accident, and these conditional probabilities are combined to provide an estimate of core damage probability. Thus, a posteriori analyses are based on the totality of operating experience having safety significance, and they are also used in the continuous search for means of improving safety. Generic data are used where plant specific data are lacking.
- The second type of analysis, termed a priori analysis, relates to a plant with no operating history (a new project on paper or a new plant in its initial stage). Here a prediction is made for a period in the future, and generic databases or models provide the basic information for the probabilistic study.

2.5. ASSESSMENT OF RESULTS

There are two basically different ways in which PSA results can be evaluated in practice.

- One possibility is to draw technical conclusions from the relative importance of the contributions to risk of different accident sequences that could be initiated by failures in plant equipment or modes of operation. These conclusions may include evaluation of the effects of improvements. Such 'relative conclusions' are of prime importance for improving safety, as they indicate the appropriateness of and the priorities for further steps to be taken.
- The other possibility is to draw conclusions about the absolute risks from a facility and about the tolerability of those risks, taking into account the associated uncertainties. Such a course requires a Level 3 PSA. In principle, this can be done both for the technical risks (probability of a severe core damage accident, probabilities of unacceptable source terms) and for the health risks that are related to such accidents.

Regarding the quality of the final judgement, the following general points can be made. Firstly, a PSA may be a combination of the a posteriori and a priori approaches in that both generic and plant specific experience is used in the database. In that case, the uncertainties will be reduced according to the extent of the a posteriori component. It is particularly important to take this into account when trying to compare the results of different PSAs. Secondly, and by definition, relative conclusions are more reliable than absolute statements. In addition, biases and uncertainties in results increase substantially from Level 1 to Level 3 assessments. It is essential that the associated range of uncertainty be quoted in conjunction with any absolute statement, and it must be accepted that the range will be so wide as to require caution in the application of the results.

2.6. MERITS OF PSA APPLICATIONS

The success of PSA in identifying vulnerabilities and possible improvements in plant safety is often closely related to the process of performing such investigations. That process opens up new opportunities to detect safety deficiencies, and it stimulates people involved to improve plant safety through careful rethinking of the entire range of possible malfunctions. That independent 'orthogonal' look at the technical system is among the most important merits of PSA methodology. It should be noted that such benefit requires a questioning attitude on the part of the analyst, all the more so because PSA lacks a strictly standardized methodology.

Altogether, PSA has proven beneficial in areas such as the following:

- evaluation of the completeness and balance of the design for safety (including the identification of risk relevant plant conditions and of possible 'cliff edge effects' with regard to accidents and their consequences);
- evaluation of modifications of plant design and procedures from a safety viewpoint;
- evaluation of management and operational strategies;
- assistance to plant management in establishing effective maintenance and testing (including 'living probabilistic safety assessments');
- training of staff;
- assistance in decision making on backfits;
- evaluation of accident management strategies;
- guidance for improving technical specifications;
- systematic monitoring of the safety level, for instance by evaluation of precursor events for their safety significance;
- establishment of priorities for future research by identification of those areas where knowledge is most incomplete, e.g. by evaluation of PSA uncertainties;
- assistance in the development of new reactor concepts.

Most of these benefits are achieved by Level 1 (core damage probability) and Level 2 (source term probability) a posteriori analyses. The success of such investigations makes them most valuable for systematic safety reviews of operating nuclear power plants.

2.7. PRECAUTIONS CURRENTLY NECESSARY IN THE USE OF PSA

Irrespective of its benefits, the use of PSA is subject to limitations. They are due to its dependence on deterministic design, to uncertainties concerning data and models, to difficulties in properly treating some issues, and to the resulting subjective views of the team performing a PSA. Such limitations must be taken into account when using PSA for decision making.

It should also be mentioned that there is as yet no recognized standardized PSA methodology. This lack makes it difficult to compare numerical results of different PSAs.

2.7.1. Dependence of accuracy on plant design

The accuracy of a PSA depends in a fundamental way on the design of the plant. A design with several independent lines of defence in relation to a particular fault permits derivation of data from past experience, since the reliability requirements for individual components or systems can be moderate and failure rates are thus observable. Where lines of defence are fewer or not fully independent, the reliability requirements must be much more stringent, and data from past experience will be scarce and highly uncertain.

Common cause failure and system interactions may play an important role. If the design based separation between systems and trains is adequately implemented, many causes for dependences, interactions and common cause failures are eliminated, and systems and trains act nearly independently of each other. This facilitates the modelling and lessens the vulnerability of the plant, systems and components to these failures. However, if such provisions are not made in the design, the vulnerability to common cause failure and complex system interactions might be large and difficult to assess.

Plant design also affects the accuracy of a PSA through the measures taken to reduce dependence on satisfactory operator performance, since human reliability is inherently difficult to quantify.

2.7.2. Uncertainty

Most PSAs include only internal initiators. They exclude external events such as earthquakes or flooding due to storms or tsunamis. INSAG does not refer to these sources of uncertainty at this point.

Much of the uncertainty in data can be estimated. However, when failures in components of nuclear plants lead to actions to prevent their recurrence, the influence of such corrections on reliability might be difficult to evaluate.

The limited capability to model with reasonable accuracy some relevant issues (e.g. phenomena of accident progression including core melt, human behaviour, health effects of low level radiation) also contributes to the uncertainty of PSA results. Such uncertainties are sometimes estimated by expert opinion.

Both types of uncertainties can be propagated through the steps of the analysis, leading to probability distributions of the calculated results. According to the presently available Level 1 PSAs of proven reactor designs, the uncertainties (90% confidence interval) in predictions of core damage probability cover a range of roughly one order of magnitude. In Level 2 analyses, the uncertainties are much larger, because of the difficulties in modelling containment loads and containment failure mechanisms associated with severe accidents. Available results show that the uncertainty range of Level 2 results can extend over several orders of magnitude. In Level 3 analyses, somewhat more uncertainty is added by the inclusion of atmospheric dispersion and of low-dose-response relationships in the evaluation of the significance of relatively few health effects in large populations. Limitations of this kind must be recognized in the application of PSA.

2.7.3. Limitation of scope

PSA is limited to certain classes of issues. Issues may be neglected because they are believed unimportant. (Such issues may begin to contribute when the importance of other issues is reduced by improvements in technology.) Issues may also be neglected because they cannot be readily included in the structure of PSA models. For instance, the scope of accident sequence analysis is generally limited to component failures of specific types and to operator failures to correctly perform described actions. The consideration of initiating events is also limited in scope. As just stated, most PSAs do not include external events as initiators. This point is discussed further in Section 2.7.7.

In the following, specific limitations of scope are described in more detail.

2.7.4. Human factors

It is difficult to model human behaviour. Thus the influence of the human factor is among the issues most difficult to quantify in a PSA. Designs whose safety largely depends on human intervention are particularly sensitive in this regard.

For proven designs, the influence of human error has been substantially reduced by automation and an improved man–machine interface. However, as the overall reliability of plant technology is constantly being improved, human error, even if reduced in absolute terms, remains an important contributor to risk.

A particular problem is the assessment of the type and probability of operator errors of commission. Those errors would be intentional acts by operators outside of procedures, which could occur as a result of vagueness of procedures, misleading instrumentation or simply errors on the part of the operators. Including such errors in a PSA is extremely difficult, because the number of possible actions to be considered is almost unlimited. Some kinds of such errors, i.e. misdiagnosis with related erroneous operator actions, are dealt with in some recent PSAs. On the whole, however, the capability to model human factors is still limited, and the results have large uncertainties. Even if such actions can be identified, quantification is difficult. Greater progress has been made in studying human response with reactor simulators; however, there may also be a systematic bias in results obtained this way, because the stress that would be present under actual conditions is absent.

2.7.5. Common cause failures

Common cause failures of redundant safety systems are observed extremely rarely, largely owing to the high quality of nuclear power plant equipment. Nevertheless, common cause failures may have a major influence on system failure rate in a highly redundant system.

There are several models in use to assess the probability of common cause failures. Most of them use existing information about single failure events in order to formulate conjectures about multiple failure probabilities. Sometimes, additional information about specific common cause events (such as double or triple failure events) is evaluated. However, there exists a basic difficulty in extrapolating these data to multiple failure probabilities, as there is in most cases no clear causal dependence between the observations and the multiple failure modes that are to be analysed. In particular for highly redundant systems (e.g. safety relief systems in boiling water reactors (BWRs)), it is therefore extremely difficult to reliably assess the failure probabilities.

This difficulty in accurately predicting common cause failure probabilities is believed to result, in many cases, in overestimation of common cause contributions. Nevertheless, because of the large uncertainty in the prediction of such effects, the potential for and consequences of common cause failure need to be addressed, and more emphasis on diversity in systems seems justified.

2.7.6. Low probability events

In general, event families of very low probability are neglected because of judgement of their unimportance. In this regard, it is common practice (and seems to be without significant influence on the outcome of an analysis) to discount event families that occur with probabilities that are two or three orders of magnitude lower than the overall probability of the postulated adverse outcome. As most PSAs of

proven reactor designs predict core damage probabilities of between 10^{-5} and 10^{-4} per reactor-year, a cut-off probability of 10^{-7} per reactor-year seems appropriate in this regard. If a total core damage probability is found to be significantly below 10^{-5} per reactor-year, issues that would be outside the scope of PSAs on the aforementioned basis may become significant if they are numerous.

The end results of a PSA represent degrees of belief that certain specified detrimental effects will occur in a given time frame. That degree of belief is described by probabilities which may be based on two different types of information:

- The first type of information is empirical data and their stochastic variability. The corresponding input into a PSA can be interpreted as the probabilities of occurrence of certain phenomena observed.
- Information of the second type is judgement about relevant issues such as phenomena, failure modes and related probabilities. Such judgements may be based upon scientific background and engineering experience, but are not directly supported by empirical data such as probabilities of occurrence.

It is a basic aim of PSA to derive the results to the largest possible extent from empirical data. As explained earlier, that is accomplished by a breakdown of the possible failure mechanisms into the product of various independent submechanisms, which permits deducing even very low accident probabilities from limited operating experience. The need to use such a method is a direct result of the success of defence in depth in nuclear plant safety. However, the share of subjective elements in results increases as the probabilities representing the end results decrease. Below a certain level of probability, the empirical component of the results will be negligible, and the PSA results will essentially be a judgement that the outcome in mind is impossible. Experience with existing PSAs of proven designs indicates that frequencies below 10^{-7} per reactor-year for event families are well below that level.

For families of events that would threaten the containment and could therefore lead directly to a large release, it might be necessary to consider even lower probabilities. However, it is useful to consider such events in a separate analysis from that for events for which the containment provides a further barrier (see Section 4).

2.7.7. Plant internal and plant external hazards

Typical hazards such as seismic events, fires and flooding (external, internal), which might compromise several safety systems simultaneously, are treated in some recent PSAs and have frequently given significant contributions to severe accident probabilities. They are clearly distinct in nature from initiators that would be associated with a localized part of the plant. They are rather predecessors of accident initiators than initiators themselves.

The contribution of those hazards to risk is site and plant specific. Relatively large contributions have sometimes been found for older plants, due to vulnerable

or non-existent physical protection and separation. In new designs, qualification of components to withstand harsh environments and adequate physical separation significantly diminish the vulnerability to hazards.

The methods presently used for assessing hazards are characterized by large uncertainties. Confidence intervals extend over several orders of magnitude even for Level 1 analyses. Such uncertainties make it meaningless to combine these results with those of events due to localized initiators.

2.7.8. Interaction between designers and operators and the PSA team

Effective use of PSA depends on the premise that the evaluation is as close as possible to reality. That requires complete information about possible failure modes and the use of best estimate data. It generally requires much more effort and better knowledge than using design data from the licensing process. It also requires keeping data up to date when modifications are made to the plants.

It is evident that the establishment and maintenance of such an information base and database can only be achieved by close co-operation between the team performing the PSA, the operator and the designer of the plant. For instance, PSA teams need free access to all relevant information from periodic tests, maintenance and repair. Walk-through of the plant by members of the PSA team is important so that they can become familiar with ongoing developments and changes in the plants and can receive dependable information about other relevant aspects of operation. Co-operation with the plant designer must support understanding of realistic system response under accident conditions and, in particular, beyond design limits. On the other hand, involvement of the plant operator and designer in PSAs furthers safety consciousness and a risk attentive attitude on the part of the staff and can thus essentially contribute to safety culture. Thus the flow of information and the benefit are in both directions: one direction improves the PSA; the other contributes to safer design and operation.

3. FURTHER DEVELOPMENT OF METHODOLOGY

The precautions currently necessary in the use of PSA are related to the availability and quality of data and to the appropriateness of models as well as to the completeness and the quality of analyses. Improvements seem possible in all fields. The following aspects are of particular importance in this regard.

3.1. PLANT DATA

Many PSAs still use a large amount of generic data for the probabilities of accident initiators and for component reliabilities. Improved collection of plant specific data and a more widespread use of methods such as the Bayes approach to combine plant specific observations with generic data should become common practice. In addition, the analysis of subtle statistical and probabilistic correlations still needs further development. Such correlations may be related to hidden deficiencies in components, for instance due to errors in manufacture, installation, inspection or maintenance.

3.2. ACCIDENT PROGRESSION MODELS

The events occurring if an accident were to progress to severe core damage and beyond would be physically and chemically complex. To date, no validated mechanistic computer codes are available to consistently model the relevant phenomena with satisfactory model accuracy and predictive capability. This holds in particular for phenomena expected to occur in the containment after vessel breach. Effort to develop adequate models should be sustained. In addition, design improvements would assist in reducing the large uncertainties of Level 2 analyses, such as the conditional probabilities of containment failure and release modes.

3.3. CONDITIONS WHILE THE PLANT IS SHUT DOWN

Until recently, virtually all PSAs for power reactors were performed for full power conditions. This was considered to be a conservative approach, based on having the maximum amount of energy available in the core, which maximizes the system response requirements and minimizes the time available to prevent damage. However, during shutdown major maintenance activities related to safety systems might be performed; the redundancy usually required at full power may not exist; emergency operating procedures may be limited; the state of the plant may be less clear owing to the many activities under way; the integrity of the primary cooling

system and that of the containment might be compromised; and the operating and maintenance staff may be expected to be less attentive. The human factor, especially in errors of commission, may be very important under those conditions. Therefore, shutdown conditions could make significant contributions to the core damage probability. Inclusion of such states in PSAs will require substantial effort, as has been seen in PSAs recently conducted in France, because within each different plant operating mode different technical specifications apply, reliability data might be different and scarce, and therefore separate analyses are required.

3.4. HUMAN FACTORS

The difficulty in modelling human behaviour is due to the lack of good data, the shortcomings in describing human actions by models and the dependence on circumstances.

Thus, it is important to improve the collection of human factor data from operating experience. Such a collection should include data on maintenance and repair. Increased use of full scale simulators would be helpful in strengthening the base of the information about human response during potential accidents, though the reservation mentioned earlier in this connection remains important.

Reduction of uncertainties from human factors will follow the development of designs that make safety less dependent on human action and the modification of existing designs to such an end, and the accumulation of greater operating experience that includes the effect of human errors.

3.5. COMMON CAUSE FAILURES

It has been stated before that data on multiple failures are extremely scarce. Therefore, significant improvement in the quantification of probabilities of common cause failure events depends on both investigating all available data on phenomena with a potential for resulting in a common cause failure, and developing common cause models emphasizing the causal dependence of common cause failure probabilities on such phenomena.

3.6. CONSIDERATION OF TIME DEPENDENCE

To date, only a few time dependent phenomena are modelled in PSA studies. Exceptions are time dependent success criteria in long term accident sequences in French PSAs. The effects of several time dependent phenomena such as ageing of components, and time dependent unavailabilities (test intervals, latent failures,

repair) and time dependences of accident sequences (time dependent success criteria, time dependent operator actions, time dependent physical phenomena) are usually treated by averaging in PSAs.

For some time dependent phenomena, such as dependence of recovery actions on time available and varying minimum success requirements, more sophisticated models should be developed. These issues, however, are not the most urgent problems in PSA, and they may be regarded more as mid-term priorities.

3.7. QUALITY ASSURANCE

Quality assurance of PSA is important, as PSA will be more widely used in the future. Careful peer review is an essential part of the review process in each case, in order to ensure that PSAs correspond to the 'state of the art'.

4. GUIDELINES FOR PRESENTATION AND INTERPRETATION OF PSA RESULTS

PSA's complex methodology is difficult for non-specialists to understand. Findings can easily be misunderstood. Therefore, presentation of results should be made as 'transparent' as possible, and should include presentation of uncertainties, scope and coverage, omitted phenomena, the peer review process, and guidance on the use of the results.

As explained in Section 2.7.6, PSA results generally lose their meaning below a certain level of probability, especially if they are related to single event families. It has also been said before that this level depends on both deterministic design and data from operating experience, and the lower level for proven designs is currently assumed to be in the range of 10^{-7} per reactor-year. As stated earlier, inclusion of events above this threshold leads to confidence in overall accuracy above 10^{-5} per reactor-year. Results related to probabilities below that threshold should generally be excluded from presentation.

Estimates of uncertainties can be among the important findings of probabilistic assessments. Therefore, it seems reasonable to depict the dependence of uncertainties on technical issues (uncertainty profiles) and the sensitivities of results to imperfectly understood phenomena.

The assessment of a risk contribution from a single event with consequential failure of all levels of defence will normally rely on a small probability of occurrence of just one phenomenon or of a group of closely related phenomena. It has been explained earlier (Sections 2.7.1 and 2.7.2) that in such a case, a calculated probability of resultant severe off-site consequences is highly uncertain and may even be, at least below a certain level of probability, rather speculative[1]. It is evident that such events should be excluded by design. If they are not, they need to be addressed in a PSA. However, such results should be presented separately from other results because of their different character and the eventual need for specific actions.

[1] The Chernobyl plant, as it was before the accident in 1986, may serve as example. That design permitted the triggering of an autocatalytic excursion with destruction of all barriers by malfunctioning of a single system, i.e. the reactivity control system. Thus, if a probabilistic assessment had been made, the calculated probability of severe consequences would have depended almost exclusively on terms such as a common cause failure of the control system or a human error.

5. HOW SHOULD PSA BE USED IN THE FUTURE?

5.1. USE FOR TECHNICAL CONCLUSIONS

The success of Level 1 PSA in a posteriori analyses being taken into account, an expanded use in this field promises further benefits. Increased use of plant specific analyses would be helpful. Further, PSA could be applied more intensely to systematic monitoring of safety. Plant personnel should be involved in those activities in order to promote the thought processes of PSA among the staff of nuclear facilities. Owing to the fact that Level 1 results can be translated relatively easily into technical findings, many PSAs are restricted to that level. Nevertheless, the integrity of the containment is highly relevant to the fundamental objective of nuclear safety, i.e. the protection of the public against radiation hazards from accidents in nuclear facilities. Therefore, PSA results should include at least the presentation of major conclusions with regard to the containment, especially if these depend significantly on specific event sequences and phenomena.

Some standardization might be required to ensure that decision making has an equivalent basis for different plants. That requires PSA guidelines[2] to define methodology standardized according to the state of the art. However, PSA methodology has not yet been perfected, and a questioning attitude when conducting a PSA is a significant contributor to safety. Therefore, such guidelines are to be adapted from time to time to the evolution of PSA, which should be advanced by non-standardized 'exploratory investigations' in depth.

5.2. USE IN CONNECTION WITH SAFETY CRITERIA

Various deterministic criteria are used for NPP design in different countries. International co-operation in the nuclear industry and the need to explain transborder safety levels clearly to the public require a more consistent international approach in that area. Probabilistic assessments could provide an essential contribution in making deterministic criteria more consistent, more 'transparent' and more comparable. However, care should be taken to maintain the distinction between a priori and a posteriori assessments.

5.3. USE FOR CONCLUSIONS ABOUT TOLERABILITY

As noted in Section 2.5, PSA results can be used either to determine the significance of different contributors to accidents or to judge the risks from a nuclear

[2] See, for example, Ref. [7] and references contained therein.

power plant. In the latter regard, it is widely accepted that decisions concerning the tolerability of risk should be based on three principles:

— There exist levels of risk from technology to individuals or society that should not be tolerated irrespective of the technology's benefits. Such levels are often referred to as tolerability limits.
— At risks lower than that level, safety cannot be absolute, and the knowledge of how to improve it is never complete. Responsible action includes continued striving for risk reduction, provided that the effort to achieve these improvements is not unreasonably high.
— Well below the tolerability limit, risks are so low that they should be regarded as negligible in order to avoid unnecessary deployment of resources which diverts attention from substantial safety issues which could lead to larger risks of other types. That corresponding low level is sometimes called a de minimis limit.

The implementation of these principles requires safety goals based on appropriate definitions of risks, which ensure that a comparison of the actual levels of risks with the goals is practicable, meaningful and 'transparent'. Goals can be set as technical safety objectives, for example on core melt probability. The corresponding criteria can be assessed using a Level 1 PSA for a core melt criterion, or a Level 2 PSA for a source term criterion. They can be related to design characteristics and potential improvements. However, to be able to proceed to comparisons with other risks, including those from other industries, goals must be set in terms of overall risks for the individuals or the society, which are called high level risk objectives[3]. In that case, a Level 3 PSA is needed, with all the associated uncertainties identified earlier.

Although this framework is likely to receive general support, achievement of an international agreement on the two values delineating the regions, tolerability limit and de minimis limit, is likely to be difficult for at least three reasons:

— it demands agreement on explicit societal risk criteria;
— it has to take into account the uncertainty margins of the PSA results;
— when comparison with other risks is sought, systematic flaws in evaluations might make the comparisons meaningless.

That holds in particular for Level 3 and a priori analyses, where the development of appropriate methods to overcome the aforementioned difficulties is an important task which will take quite some time.

On the other hand, technical objectives, such as core damage probability or probability of source terms of given sizes, are in use. The related limit values could

[3] It is understood that other factors such as land contamination must be taken into account in determining objectives for societal risks.

and should be strengthened by appropriate consideration of the problems of uncertainties in PSA results and of comparability between different PSAs. The use of confidence levels (e.g. 95% percentiles) is recommended in this regard. It also seems reasonable to establish quantitative requirements for issues difficult to assess, such as common cause failures and human errors. The definition of minimum contributions of those factors to the risk level would help to eliminate meaningless evaluations from comparisons.

6. CONCLUSIONS

Nuclear power plants are generally designed to deterministic requirements. Nevertheless, many probabilistic assessments have now been carried out on existing plants and proposed designs. Numerous lessons have been learned from these applications, and there is now a considerable and continuously increasing knowledge base on the capabilities and the limits of PSA.

Thus it can be said that PSA has matured to a point where there is now a broad basis of understanding. There is agreement that it constitutes a valuable additional basis for safety assessment and for decisions on safety improvements. In particular, the methodology has proven to be a most valuable tool for identification of plant weaknesses.

The use of PSA is therefore strongly encouraged. Plant operators and plant operating personnel should be involved in these activities. However, the methodological limitations and the range of uncertainties involved must be taken into account in the interpretation and use of results.

With appropriate caution, PSA has applicability in safety analysis, plant design, control of operating practices and licensing. Another important area where past applications have been found useful, and where future activities are strongly encouraged, is the use of PSA for evaluation of operating experience (e.g. precursor analyses).

It is essential that uncertainties should be emphasized in displaying results. The presentation of point estimates should be restricted as far as possible, and uncertainties should be reflected even in that case. It must also be recognized that PSA results change their character and lose their meaning below a certain level of probability. In special cases, if new phenomena are involved, a separate presentation of low probability results might be warranted. In general, however, results should not be displayed if probabilities are below a level in the range of 10^{-7} per reactor-year.

Particular attention to the possibility of biases and uncertainties due to subjective views of PSA teams, human factor and common cause contributions, dependence of accuracy on deterministic design, and uncertainties related to modelling containment loads and off-site consequences is required when interpreting PSA results. It must also be recognized that the uncertainties of results escalate greatly for a PSA beyond Level 1. Furthermore, the extent to which external events have been included among the initiators must be borne in mind.

The use of PSA for the establishment of acceptance criteria has turned out to be difficult. That is due to both the difficulty in completely assessing all biases and uncertainties in numerical terms and to the dependence of acceptance safety levels on a number of factors, such as expected lifetime, perceived risk, availability of data, ability to carry out realistic calculations and the methods used in the original design.

Nevertheless, it is necessary to establish assessment criteria in order to identify to what extent resources should be spent in continuing to reduce risks. In this regard,

fundamental risk criteria (health effects) are most readily comparable and in spite of the problems attached to higher uncertainties they provide the opportunity to base such decisions on a footing comparable with that applied in other areas of life. However, intermediate technical surrogates are often more useful as their probabilities can be calculated more precisely with PSA. There is an emerging international consensus on target probabilities of core damage and large accidental release.

There have been differences in the methodologies used in PSAs, and there is a definite need for improvement in methods and data. In particular, for future reactors for which utilities and regulators may wish to compare an international range of designs there is a clear need to agree on consistent methodology and assessment criteria in order to ensure that comparisons are valid. Such standardized procedures should be subject to periodic review as PSA methodology is not sufficiently mature for its present status to be frozen.

Important areas requiring further effort in methodology include human factors, common cause failures, hazards analysis, and low probability cut-off levels. Efforts in data collection should be strengthened in order to improve modelling in these areas and to extend the use of plant specific PSA. Attention should also be given to extended application of PSA in areas such as identification of relevant research issues, and training of plant personnel and regulatory staff. A further important issue is improving communication on PSA and risk among nuclear engineers and scientists, scientists in other fields, and the general public. All of these activities need international co-operation and co-ordination.

REFERENCES

[1] RASMUSSEN, N.C., Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants, Main Report, Rep. WASH-1400-MR (NUREG-75/014), United States Nuclear Regulatory Commission, Washington, DC (1975).

[2] BUNDESMINISTER FÜR FORSCHUNG UND TECHNOLOGIE, Deutsche Risikostudie — Kernkraftwerke, TÜV Rheinland, Cologne (1979).

[3] GESELLSCHAFT FÜR REAKTORSICHERHEIT, Deutsche Risikostudie — Kernkraftwerke: Phase B, GRS, Cologne (1989).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, The Role of Probabilistic Safety Assessment and Probabilistic Safety Criteria in Nuclear Power Plant Safety, Safety Series No. 106, IAEA, Vienna (1992).

[5] KOUTS, H.J.C., et al., Special Committee Review of the Nuclear Regulatory Commission's Severe Accident Risks Report (NUREG-1150), Rep. NUREG-1420, United States Nuclear Regulatory Commission, Washington, DC (1990).

[6] NUCLEAR REGULATORY COMMISSION, Severe Accident Risks: An Assessment for Five US Nuclear Power Plants, Final Summary Report, 3 vols, Rep. NUREG-1150, Washington, DC (1990).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants, Safety Series No. 50-P-4, IAEA, Vienna (1992).

MEMBERS OF THE INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP

Beninson, D.
Birkhofer, A.
Chatterjee, S.K.
Domaratzki, Z.
Edmondson, B.
González-Gómez, E.
Kouts, H.J.C. (Chairman)
Lepecki, W.
Li, Deping
Sato, K.
Sidorenko, V.A.
Tanguy, P.
Vuorinen, A.P.

HOW TO ORDER IAEA PUBLICATIONS

An exclusive sales agent for IAEA publications, to whom all orders and inquiries should be addressed, has been appointed for the following countries:

CANADA UNITED STATES OF AMERICA	UNIPUB, 4611-F Assembly Drive, Lanham, MD 20706-4391, USA

In the following countries IAEA publications may be purchased from the sales agents or booksellers listed or through major local booksellers. Payment can be made in local currency or with UNESCO coupons.

ARGENTINA	Comisión Nacional de Energía Atómica, Avenida del Libertador 8250, RA-1429 Buenos Aires
AUSTRALIA	Hunter Publications, 58 A Gipps Street, Collingwood, Victoria 3066
BELGIUM	Service Courrier UNESCO, 202, Avenue du Roi, B-1060 Brussels
CHILE	Comisión Chilena de Energía Nuclear, Venta de Publicaciones, Amunategui 95, Casilla 188-D, Santiago
CHINA	IAEA Publications in Chinese: China Nuclear Energy Industry Corporation, Translation Section, P.O. Box 2103, Beijing IAEA Publications other than in Chinese: China National Publications Import & Export Corporation, Deutsche Abteilung, P.O. Box 88, Beijing
CZECHOSLOVAKIA	S.N.T.L., Mikulandska 4, CS-116 86 Prague 1 Alfa, Publishers, Hurbanovo námestie 3, CS-815 89 Bratislava
FRANCE	Office International de Documentation et Librairie, 48, rue Gay-Lussac, F-75240 Paris Cedex 05
HUNGARY	Kultura, Hungarian Foreign Trading Company, P.O. Box 149, H-1389 Budapest 62
INDIA	Oxford Book and Stationery Co., 17, Park Street, Calcutta-700 016 Oxford Book and Stationery Co., Scindia House, New Delhi-110 001
ISRAEL	YOZMOT (1989) Ltd, P.O. Box 56055, Tel Aviv 61560
ITALY	Libreria Scientifica, Dott. Lucio de Biasio "aeiou", Via Meravigli 16, I-20123 Milan
JAPAN	Maruzen Company, Ltd, P.O. Box 5050, 100-31 Tokyo International
PAKISTAN	Mirza Book Agency, 65, Shahrah Quaid-e-Azam, P.O. Box 729, Lahore 3
POLAND	Ars Polona-Ruch, Centrala Handlu Zagranicznego, Krakowskie Przedmiescie 7, PL-00-068 Warsaw
ROMANIA	Ilexim, P.O. Box 136-137, Bucharest
RUSSIAN FEDERATION	Mezhdunarodnaya Kniga, Smolenskaya-Sennaya 32-34, Moscow G-200
SOUTH AFRICA	Van Schaik Bookstore (Pty) Ltd, P.O. Box 724, Pretoria 0001
SPAIN	Díaz de Santos, Lagasca 95, E-28006 Madrid Díaz de Santos, Balmes 417, E-08022 Barcelona
SWEDEN	AB Fritzes Kungl. Hovbokhandel, Fredsgatan 2, P.O. Box 16356, S-103 27 Stockholm
UNITED KINGDOM	HMSO, Publications Centre, Agency Section, 51 Nine Elms Lane, London SW8 5DR
YUGOSLAVIA	Jugoslavenska Knjiga, Terazije 27, P.O. Box 36, YU-11001 Belgrade

---

Orders from countries where sales agents have not yet been appointed and requests for information should be addressed directly to:

Division of Publications
International Atomic Energy Agency
Wagramerstrasse 5, P.O. Box 100, A-1400 Vienna, Austria

92-01184

ISBN 92-0-102492-4