Nuclear Safety ISBN 92-64-01047-5

CSNI Technical Opinion Papers

No. 7:

Living PSA and its Use
in the Nuclear Safety Decision-making Process

No. 8:

Development and Use of Risk Monitors
at Nuclear Power Plants

NEA No. 4411

NUCLEAR ENERGY AGENCY
ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 30 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

* * *

This work is published on the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Organisation or of the governments of its member countries.

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1st February 1958 under the name of the OEEC European Nuclear Energy Agency. It received its present designation on 20th April 1972, when Japan became its first non-European full member. NEA membership today consists of 28 OECD member countries: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Portugal, the Republic of Korea, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities also takes part in the work of the Agency.

The mission of the NEA is:

- to assist its member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally friendly and economical use of nuclear energy for peaceful purposes, as well as
- to provide authoritative assessments and to forge common understandings on key issues as input to government decisions on nuclear energy policy and to broader OECD policy analyses in areas such as energy and sustainable development.

Specific areas of competence of the NEA include safety and regulation of nuclear activities, radioactive waste management, radiological protection, nuclear science, economic and technical analyses of the nuclear fuel cycle, nuclear law and liability, and public information. The NEA Data Bank provides nuclear data and computer program services for participating countries.

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

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The Committee on the Safety of Nuclear Installations (CSNI) of the OECD Nuclear Energy Agency (NEA) is an international committee made up of senior scientists and engineers. It was set up in 1973 to develop, and co-ordinate the activities of the Nuclear Energy Agency concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations. The Committee's purpose is to foster international co-operation in nuclear safety among the OECD member countries.

The CSNI constitutes a forum for the exchange of technical information and for collaboration between organisations, which can contribute, from their respective backgrounds in research, development, engineering or regulation, to these activities and to the definition of the programme of work. It also reviews the state of knowledge on selected topics on nuclear safety technology and safety assessment, including operating experience. It initiates and conducts programmes identified by these reviews and assessments in order to overcome discrepancies, develop improvements and reach international consensus on technical issues of common interest. It promotes the co-ordination of work in different member countries including the establishment of co-operative research projects and assists in the feedback of the results to participating organisations. Full use is also made of traditional methods of co-operation, such as information exchanges, establishment of working groups, and organisation of conferences and specialist meetings.

The greater part of the CSNI's current programme is concerned with the technology of water reactors. The principal areas covered are operating experience and the human factor, reactor coolant system behaviour, various aspects of reactor component integrity, the phenomenology of radioactive releases in reactor accidents and their confinement, containment performance, risk assessment, and severe accidents. The Committee also studies the safety of the nuclear fuel cycle, conducts periodic surveys of the reactor safety research programmes and operates an international mechanism for exchanging reports on safety related nuclear power plant accidents.

In implementing its programme, the CSNI establishes co-operative mechanisms with NEA's Committee on Nuclear Regulatory Activities (CNRA), responsible for the activities of the Agency concerning the regulation, licensing and inspection of nuclear installations with regard to safety. It also co-operates with NEA's Committee on Radiation Protection and Public Health and NEA's Radioactive Waste Management Committee on matters of common interest.

* * * * * * * * * * * *

Requests for additional copies of this report should be addressed to:

Nuclear Safety Division
OECD Nuclear Energy Agency
Le Seine St-Germain
12 blvd. des Iles
92130 Issy-les-Moulineaux,
France

FOREWORD

The main mission of the NEA Committee on the Safety of Nuclear Installations (CSNI) Working Group on Risk Assessment (WGRisk) is to advance the understanding and utilisation of probabilistic safety analysis (PSA) in ensuring the continued safety of nuclear installations and in improving the effectiveness of regulatory practices in NEA member countries. In pursuing this goal, the Working Group examines the different methodologies for identifying contributors to risk and assessing their importance, while continuing to focus on the more mature PSA methodologies for Level 1, Level 2, internal and external events, and shutdown conditions. It also considers the applicability and maturity of PSA methods for addressing evolving issues such as human reliability, software reliability and ageing issues, as appropriate.

Technical opinion papers are considered to be one of the most important products produced by the WGRisk, and as such are produced in conjunction with the issuance of any new report, the completion of a workshop or following in-depth discussions. Recent technical opinion papers have addressed human reliability analysis, fire probabilistic safety analysis and seismic probabilistic safety analysis.

The technical opinion paper on living PSA resulted from several in-depth discussions held by the WGRisk following the issuance of a report on the state of the art. The technical opinion paper on risk monitors is the outcome of a joint task between the WGRisk and the International Atomic Energy Agency (IAEA). It was developed using the results from an international workshop and a state-of-the-art report being produced this year.

The NEA Secretariat wishes to express particular thanks to Dr. Charles Shepherd, WGRisk task leader and the main author of these two papers, who contributed valuable time and considerable knowledge to their preparation. Thanks are also extended to the members of the WGRisk and participants in the IAEA consultants meetings for their valuable insights, which provided much of the foundation for this work. In this regard, Dr. Javier Yllera provided excellent co-operation and assistance on behalf of the IAEA.

PERSPECTIVE

From the Chairman of CSNI, Mr. Ashok Thadani:

The PSAs for many of the nuclear power plants throughout the world are being maintained as living PSAs (LPSAs) so that they are being updated to take account of changes to the design and operation of the plant, improvements in the understanding of how the plant behaves in fault conditions, and improved PSA methods, models and data. These LPSAs are being routinely used as one of the inputs into an integrated decision-making process where requirements from the deterministic analysis, PSA and other requirements (such as legal and regulatory requirements) are weighted and combined in order to provide a sound and auditable justification for any decisions made on plant nuclear safety issues.

One of the specific applications of a LPSA is the risk monitor and these are being used by operators and regulators to provide risk information for use in the decision-making process to ensure the safe operation of nuclear power plants. Since the first risk monitors were put into operation in 1988, the number of risk monitors worldwide has increased rapidly so that by the end of 2003 there were more that 110 in operation and this should increase to over 150 when those being developed are placed in service.

Although the PSA model used in the risk monitor is based on the LPSA model, it is important to realise that this may not be directly usable as a risk monitor PSA for a number of reasons. The aim of the risk monitor is to provide an estimate of the point-in-time risk for the current plant configuration and environmental factors whereas the LPSA provides an estimate of the average risk hence uses average initiating event frequencies and maintenance unavailabilities, and usually takes account of the exposure time to different initiating events as the plant passes through the different plant operational states modelled in the PSA. Hence, the LPSA model needs to be reviewed for any average or assumed conditions in the model to ensure that an accurate point-in-time risk is calculated for all configurations.

Combining these two technical opinion papers into a single document provides the reader, in this case ranging from decision makers in the nuclear community, regulators, nuclear power plant operators, etc., the opportunity to have a concise assessment of the current state of the art to enable better analysis when evaluating proposals or development of these applications.

Finally, although PSA is a powerful integral tool, one needs to note that safety decisions need to carefully weigh any limitations in scope and uncertainties (parameter and model) in the PSA model.

TABLE OF CONTENTS

TECHNICAL OPINION PAPER No. 7

Living PSA and its Use in the Nuclear Safety Decision-making Process

TECHNICAL OPINION PAPER ON LIVING PSA AND ITS USE IN THE NUCLEAR SAFETY DECISION-MAKING PROCESS

Introduction

This technical opinion paper presents the consensus of risk analysts and experts in the NEA member countries on the state of the art for the production and use of living probabilistic safety analysis (LPSA) in the safety decision-making process for nuclear power plants. The objective is to present a clear technical opinion to a wide audience ranging from decision makers in the nuclear community, regulators, nuclear power plant operators, professionals working in the field of nuclear safety and PSA, and the general public.

Background

Based on a large number of successful applications around the world over many years, it is clear that PSA is mature enough for routine use in the safety decision-making process for nuclear power plants by both plant operators and Regulatory Authorities. The current practice is to apply an integrated decision-making process where the legal and regulatory requirements, insights from the deterministic analysis, insights from the PSA and other information (such as the results of a cost-benefit analysis) are weighted and combined to provide a sound and auditable basis for any decisions made on plant nuclear safety issues.

Any PSA that is carried out will reflect the design and operation of the plant, the understanding of how the plant behaves in fault conditions and the data available at the time the analysis was carried out. However, the basis for the PSA will change with time due to physical changes in the design of the plant, changes in the way that the plant is operated, improvements in the understanding of how the plant would behave in fault conditions and the availability of more plant specific data. To ensure that the PSA continues to provide a valid input into the decision-making process, it must be kept up to date to reflect these changes to the plant and take account of improvements in PSA methods. This leads to the concept of a living PSA. The emerging

standard is for the PSAs for nuclear power plants to be maintained as living PSAs and for them to be used to provide the risk information required by the integrated decision-making process.

LPSA has been the subject of a series of workshops organised by the NEA [1]. This technical opinion paper reflects the current best practice in LPSA which has emerged from these workshops and subsequent exchanges of information between the NEA member countries [2].

Definition of a LPSA

The first requirement is that a high quality PSA has been developed for the plant. It is good practice for the PSA to be done in a way that is consistent with the current guidance and standards on PSA practices, models and methods. This could include national standards, guidance produced by international organisations such as OECD and IAEA, and standards being produced by organisations such as ASME. In addition, the quality, scope and level of detail of the PSA needs to be adequate for its proposed applications and for it to have gone through a rigorous, independent peer review process.

This can then be used as the basis for the LPSA which is defined by IAEA as: "a PSA of the plant, which is updated as necessary to reflect the current design and operational features, and is documented in such a way that each aspect of the model can be directly related to existing plant information, plant documentation or the analysts' assumptions in the absence of such information. The LPSA would be used by designers, utility and regulatory personnel for a variety of purposes according to their needs, such as design verification, assessment of potential changes to the plant design or operation, design of training programs and assessment of changes to the plant licensing basis" [3].

The important aspects of this definition are that the PSA is:

- updated as necessary to maintain it as a living analysis;
- consistent with the current design and operation of the plant which may be changed as modifications are made;
- documented so that the analysis can be traced back to the plant information and analysts' assumptions;
- in a form that can be used by designers, utility and regulatory personnel which would be done off-line by PSA specialists; and

- useable for a variety of purposes that would include a range of risk-informed applications.

Hence, maintaining the PSA as a living PSA will provide a better understanding of the level of safety of the plant and how this is affected by changes to the design or operation of the plant, improvements in the PSA modelling and changes in the data used to quantify the PSA.

Reasons for requiring a LPSA

The basis for the PSA will change with time for a number of reasons. To ensure that the PSA continues to provide a valid input into the decision-making process, it must be kept up to date to reflect these changes which could include the following:

- **Changes to the design or operation of the plant**: Many such changes are made over the lifetime of a nuclear plant. In general, they will lead to a reduction in the level of risk from the plant – for example, where additional equipment is provided for carrying out plant safety functions. However, some of them may lead to an increase in the risk (where this is allowed by the Regulatory Authority) – for example, where the power level of the reactor is increased.
- **Changes in the understanding of how the plant behaves in fault conditions**: This could come from new transient analysis that changes the way that the operation of the safety systems need to be modelled in the PSA, severe accident analysis that changes the understanding of how the containment would be expected to behave following core damage, and feedback from operating experience or simulator training.
- **Data derived from plant operating experience**: It is good practice for plant operators with a LPSA to collect operating experience data and to use this to update the numerical values used in the LPSA for initiating event frequencies, component failure probabilities, etc. There is a high level of involvement by NEA in the data collection for PSA [4].

- **Increases in the scope of the PSA**: It is often the case that the initial PSA addresses the contributions to the risk from internal initiating events occurring at power and, as time goes on, the scope of the analysis is extended to include the contribution to the risk from: internal hazards such as fire and flood; external hazards such as seismic events and extreme environmental conditions; other modes of operation of the plant such as low power and shutdown conditions; the behaviour of the containment following core damage (Level 2 PSA); and the off-site consequences following a release of radioactive material from the plant (Level 3 PSA).
- **Improvements in PSA methods**: In recent years, improvements have been made in PSA methods as follows: addressing the contributions to the risk from hazards such as fire and seismic events; modelling common cause failures and human errors; and incorporating human errors of commission into the PSA. The PSA may also be developed so that it can be run using one of the modern PSA computer codes.

Such improvements will increase the range of plant safety issues that can be addressed using the LPSA.

Updating the LPSA

The LPSA needs to be updated to take account of all the changes identified above. The frequency at which this is done varies for different plants. However, it is good practice to track all the changes that occur and assess their impact on the results of the PSA. If they are significant, the aim should be to update the PSA as soon as possible. If they are not significant, they should be added to the list of changes to be included in the next update. It is good practice for a plant procedure to be developed for carrying out the preliminary assessment of changes to the plant and for updating the PSA.

Maintaining a LPSA requires a team of analysts who are trained and experienced in PSA. This will require expertise to cover all aspects of the PSA including systems analysis, data, internal and external hazards, Level 1, 2 and 3 PSA, etc. In addition, support will need to be provided in thermal hydraulic analysis, severe accident analysis, fire and seismic analysis, structural analysis (to address the response of the containment to severe accidents), etc.

For the LPSA to be accepted and used in the safety decision-making process it needs to be owned by the plant staff and used as an integral part of the plant operation. Hence, it is good practice to involve the plant staff in the updating process.

Documentation of the PSA

The use of the PSA in the safety decision-making process requires that the results/conclusions/recommendations can be traced back to the design/ operation/assumptions used for the analysis. This requires that the basis for the PSA is fully documented and for this to be organised so that it is possible to trace all aspects of the PSA back to the source information. For a new PSA, it is good practice for the documentation to be organised so that this can be done easily. For an existing PSA, this would involve reorganising the documentation or, if this is not possible, providing a route map to guide the user through the existing documentation.

The documentation needs to include details of the design and operation of the plant to which the PSA model relates and details of the analysis that forms the basis for the models used in the PSA. This would include the transient analysis that provides the basis for the safety system success criteria, the severe accident analysis that forms the basis for the containment analysis in the Level 2 PSA and the off-site consequence modelling in the Level 3 PSA. This needs to be supported by the detailed calculation files.

The justification for the data used for initiating event frequencies, component failure probabilities, common cause failure probabilities, human error probabilities, etc. should be provided. The numerical values should be traceable back to the source data or models.

The suite of documentation should include the calculation files that give details of the assumptions made, the models used, the data and the results. This should be maintained as controlled documentation. There should be a sufficient level of detail to allow another analyst to understand/recreate/modify/update the analysis as required.

The experience in the NEA member countries is that the LPSA is continually in a state of evolution. In view of this, it is good practice to ensure that, at any time, there is one reference version of the LPSA available along with the corresponding documentation. In addition, all the details of the LPSA need to be documented and checked to the same level as the original PSA.

Use of the LPSA in the decision-making process

LPSA is now being used routinely in the safety decision-making process at nuclear power plants throughout the world. It is being used as part of an integrated (sometimes referred to as a risk-informed) decision-making process in which the insights from the deterministic and probabilistic approaches are combined with the other requirements in reaching a decision. In addition, LPSAs are being used as an input into the way that Regulatory Authorities carry out their activities (sometimes referred to as risk-informed regulation).

This integrated approach using the input from the LPSA may be used to support decisions made in a number of areas related to the safety of the plant which include the following:

- proposals to make changes to the design or operation of the plant;
- applications to make changes to, or get exemptions from, the plant technical specifications in areas such as allowed outage times, test intervals and allowed plant configurations;
- other risk-informed applications such as in-service inspection and graded quality assurance; and
- the analysis of operational events (precursor analysis) using the PSA to improve the understanding of the behaviour of the plant and the risk significance of failures that have occurred in service.

The aim of following the integrated approach is to ensure that all the relevant factors are identified and taken into account so that a balanced decision is made, which ensures that the defence in depth requirement is met so that there are multiple barriers to the release of radioactive material from the plant, and that sufficient safety margins are maintained.

The role of the LPSA is to provide an input into the decision-making process on the risk significance of the issue being addressed. The LPSA can be used in two ways: firstly, to provide an estimate of the overall risk from the plant – usually the core damage frequency (CDF) and sometimes the large early release frequency (LERF), and secondly to determine the change in the risk from proposed change in the design or operation of the plant.

In doing this, it needs to be recognised that there may be shortcomings in the LPSA that need to be taken into account. For example, the scope of the PSA may be limited so that it does not address the contributions to the risk from external hazards or it may not address all the modes of operation of the plant

that arise during shutdown and refuelling. In addition, the current state of the art for PSA means that some issues such as component ageing and safety culture are not explicitly addressed.

Hence, as can be seen above, the LPSA can be used for:

- long term safety planning to address changes to the design or operation of the plant including back-fitting, the optimisation of testing and preventative maintenance, and the balancing of preventative and corrective maintenance; and
- short term safety planning where the LPSA is used off-line to provide an input into safety system configuration control, exemptions from technical specifications, and the analysis of operational events using a PSA-base approach.

In addition, the LPSA can be used as the basis for a risk monitor application which can be used on-line to provide risk information relating to the actual plant configuration. However, changes usually need to be made to the LPSA to remove simplifications made in the analysis that are not appropriate for a risk monitor PSA model and to carry out enhancements to the PSA model. The aim is to ensure that the risk monitor will provide more representative estimates of the risk for all the plant configurations and environmental factors that could arise. The way that this is done is well known from many successful risk monitor applications worldwide.

Issues and limitations related to LPSAs

There may be limitations in a particular LPSA that need to be understood before it can be used correctly in the safety decision-making process during plant operation. The main limitations arise from the scope of the PSA that has been carried out. For example, the scope of the LPSA may be limited so that it does not address the contributions to the risk from all the internal and external hazards that could occur, the analysis may only be a Level 1 PSA so that it does not address the behaviour of the containment following fault sequences in which the core is damaged or the analysis may address full power operation only and not the low power and shutdown modes of the plant. The LPSA will only provide valid risk information and insights within the limits of the PSA that has been carried out so that any such limitations need to be recognised when the LPSA is used in the safety decision-making process.

Concluding remarks

The following conclusion can be drawn regarding the state of the art in the development and use of living PSAs in the safety decision-making process at nuclear power plants:

- The majority of the PSAs that have been produced for nuclear power plants in the NEA member countries are being maintained as living PSAs.

- These LPSAs are routinely updated to take account of changes to the design and operation of the plant, improvements in the understanding of how the plant behaves in fault conditions, and improvements in PSA methods, models and data.

- These LPSAs are being used routinely as one of the inputs into making decision on the safety issues that arise at nuclear power plants (referred to as risk-informed decision making) and in determining the way that regulatory authorities carry out their activities (risk-informed regulation).

- There may be shortcomings in the risk information provided by the LPSA which could arise from limitations in the scope of the LPSA. These needs to be recognised and taken into account when the risk information it provided by the LPSA is being used.

- The LPSA generally provides one of the inputs into an integrated decision-making process where the insights from the deterministic analysis, PSA and other requirements (such as legal and regulatory requirements) are weighted and combined in reaching a decision.

References

[1] *State of Living PSA and Further Developments*; NEA/CSNI/R(1999)15; 1999.

[2] *The Use and Development of Probabilistic Safety Assessment in NEA Member Countries*; NEA/CSNI/R(2002)18; July 2002.

[3] Living Probabilistic Safety Assessment (LPSA); IAEA TECDOC Series No. 1106; September 1999.

[4] *Reliability Data Collection*, Workshop Proceedings, Budapest, Hungary; NEA/CSNI/R(1998)10; April 1998.

TECHNICAL OPINION PAPER No. 8

Development and Use of Risk Monitors
at Nuclear Power Plants

TECHNICAL OPINION PAPER ON THE DEVELOPMENT AND USE OF RISK MONITORS AT NUCLEAR POWER PLANTS

Introduction

This technical opinion paper presents the consensus of risk analysts and experts in the NEA member countries on the current state of the art in the development and use of risk monitors at nuclear power plants. The objective is to present a clear technical opinion on the state of the art to a wide audience ranging from decision makers in the nuclear community, regulators, nuclear power plant operators, professionals working in the field of nuclear safety and PSA, and the general public.

Background

One of the specific applications of a living probabilistic safety analysis (LPSA) is the risk monitor and these are being used by operators and regulators to provide risk information for use in the decision-making process to ensure the safe operation of nuclear power plants.

The first risk monitors were developed in the UK and put into operation in 1988. These were the essential systems status monitor (ESSM) at Heysham 2 and ESOP1/LINKITT at Torness. Since then, the number of risk monitors worldwide has increased rapidly so that by the end of 2003 there were more that 110 in operation and this should increase to over 150 when those being developed in countries such as Japan and Korea are put into service. In addition, the number of risk monitor software packages has grown and there are about 12 in use, some of which are commercially available and other in use in particular countries or at particular plants. The state of the art in the development and use of risk monitors at nuclear power plants is described in [1] and [2].

The term risk monitor has been defined by IAEA as “a plant specific real-time analysis tool used to determine the instantaneous risk based on the actual status of the systems and components. At any given time, the risk monitor reflects the current plant configuration in terms of the known status of the various systems and/or components – for example, whether there are any

components out of service for maintenance or tests. The risk monitor model is based on, and is consistent with, the LPSA. It is updated with the same frequency as the LPSA. The risk monitor is used by the plant staff in support of operational decisions" [3].

The current trend is to base the risk monitor on a full scope PSA that addresses all internal initiating events, all internal and external hazards, addresses both the core damage frequency (CDF) and the large early release frequency (LERF), and covers all the modes of operation of the plant including power operation and the shutdown and refuelling modes. However, many of the risk monitors currently in service are based on a PSA that has a more limited scope and, where this is the case, the limitations in the risk information that it provides need to be recognised.

Although the risk monitor PSA model needs to be consistent with the LPSA in that the two models relate to the same design and operation of the plant, are based on the same requirements for safety systems to operate after initiating events and much of the same data, there are a number of differences between the two. The risk monitor is a real-time analysis tool that is used on-line to provide risk information during normal plant operation whereas the LPSA is used off-line. The risk monitor provides a calculation of the point-in-time risk (referred to as the instantaneous risk in the IAEA definition) whereas the LPSA calculates the average risk. The point-in-time risk is calculated for each plant configuration, which relates to the state of plant systems and components that are under the control of the operators and is defined in terms of the current plant alignments, component outages, activities being carried out on the plant that affect the risk and factors related to the plant operational state. This is done for each mode of operation of the plant – that is, whether it is in full power operation, low power operation or in one of the states that arise during plant shutdown and refuelling.

One of the requirements for the risk monitor is that it can be used by all the plant staff in support of operational decisions, not just the PSA specialists who use the LPSA. The overall aim is to control the plant configuration to maintain the risk within acceptable limits. Traditionally, this has been done using the deterministic rules given in the plant technical specifications. These are formulated to ensure that maintenance outages are controlled so that the safety systems have an adequate level of diversity, redundancy and defence in depth. The additional risk information provided by the risk monitor enables staff to plan maintenance to minimise risk as well as staying within the deterministic rules.

It should be noted that, to provide an estimate of the point-in-time risk, the risk monitor needs more information on the state of the plant than is used in the LPSA, and requires a different treatment of maintenance outages and system alignments. Hence, the LPSA model cannot generally be used directly for a risk monitor application and changes need to be made.

Reasons for developing a risk monitor

There have been a wide variety of reasons given for the development of risk monitors at nuclear power plants in the NEA member countries. The main one is to address the US NRC maintenance rule which requires plant operators to assess and manage the risk associated with maintenance activities, and this can be done most easily using a risk monitor. In particular, the Code of Federal Regulations 10 CFR 50.65 (a)(4) states that: "before performing maintenance activities (including but not limited to surveillance, post-maintenance testing, and corrective and preventive maintenance), the licensee shall assess and manage the increase in risk that may result from the proposed maintenance activities. The scope of the assessment may be limited to those structures, systems, and components that a risk-informed evaluation process has shown to be significant to public health and safety". This requirement applies to all the plant operational modes.

Other reasons identified include being able to apply a risk-informed approach to managing plant operational safety, being able to schedule maintenance to avoid peaks in the risk, achieving greater flexibility in plant operation, providing the justification for carrying out more maintenance on-line, providing information on the risk importance of components during maintenance activities and providing advice on which components to restore to service.

From the experience in using risk monitors in the NEA member countries, it is clear that a pro-active, on-line approach to risk management using a risk monitor has achieved greater risk reductions than plants that have taken the off-line approach. Whereas the on-line approach can prevent peaks in the risk occurring, retrospective use can only prevent peaks that have occurred in the past from re-occurring by changing the way that these maintenance activities are carried out.

Risk monitor software

The software used for a risk monitor is significantly different from that used for a LPSA. An essential difference is that the risk monitor is designed to be used by all nuclear power plant personnel rather than by PSA specialists so that no specialist knowledge would be required in fault tree and event tree modelling or any of the other techniques used in the development of the PSA. However, the updating of the PSA model and databases does require the support of PSA specialists.

Three methods have been used by risk monitor software as follows: 1) to solve the PSA model for each plant configuration, 2) to use pre-solved solutions for a wide range of plant configurations or 3) to use a cut-set manipulation technique that starts with a PSA solution that has been produced using a very low cut-off level. The emerging standard is for the risk monitor to solve the PSA model since this allows more flexibility in modelling environmental factors and provides a more representative estimate of the risk for all plant configurations. The combination of modern software and modern hardware allows this to be done very rapidly.

Uses of risk monitors

The main use of risk monitors is as an on-line tool to monitor and control the risk from the plant configurations that arise during normal plant operation, calculate and monitor the allowed configuration time as the plant configuration changes, and monitor the cumulative risk. They are also used for maintenance planning to ensure that maintenance activities are carried out in a way that prevents the occurrence of large peaks in the risk and restricts the cumulative risk over a period of time to an acceptable level.

Risk monitors are also used off-line to produce risk profiles for plant management, to investigate why peaks have occurred in the risk with a view to ensuring that this is not repeated and to carry out an analysis of unplanned events such as those caused by equipment failures. In addition, risk monitors are often used as a PSA tool since they are much easier to use than the LPSA.

Since the risk monitor provides a very clear indication of how the activities being carried out on the plant influence the risk, it is often used in training programmes as an aid to increasing risk awareness and enhancing safety culture.

The current trend in the management of nuclear power plant safety is to move towards an integrated approach that combines the risk information

provided by the risk monitor with deterministic and other requirements to ensure that the occurrence and duration of plant configurations are managed in such a way as to keep both the point-in-time and cumulative risks at or below prescribed levels while at the same time encouraging compliance with the deterministic safety management principles.

Development of the risk monitor PSA model from the LPSA

The basis for the PSA model used in the risk monitor is a LPSA that reflects the current design and operation of the plant and is of sufficient quality, scope and level of detail to support this PSA application.

However, the LPSA is not useable directly in the risk monitor and changes typically need to be made to remove the simplifications made in the analysis that are not suitable for the risk monitor application. For example, the LPSA usually assumes one system alignment and one configuration of running and standby trains for normally operating systems. The PSA model needs to be changed to ensure that the likely plant configurations are modelled accurately and the correct component failure modes are included.

Enhancements may also need to be made to the LPSA. This often includes improvements in the way that common cause failures (CCFs) and human error probabilities (HEPs) are modelled so that they relate to the actual plant configuration entered. In addition, changes may be made to initiating event frequencies and basic event probabilities to take account of environmental factors – for example, to model the increase in the frequency of loss of off-site power during adverse weather conditions or during switchgear maintenance activities.

In making these changes, the aim is to ensure that the risk monitor will provide more representative estimates of the risk for all the plant configurations and environmental factors that could arise. The way that this is done is well known from many successful risk monitor applications in the NEA member countries.

Validation of the risk monitor PSA model

Since a large number of changes often need to be made to the LPSA model and data before it can be used in a risk monitor, there is a need for a rigorous validation process to be carried out. This needs to check that the quantitative results produced by the risk monitor PSA are consistent with (or equivalent to) those from the LPSA. The validation process needs to cover all the changes made to the LPSA model and data, and check that correct results are produced for alignments not addressed in the LPSA.

The validation process needs to be of sufficient rigour to ensure that an accurate result is obtained for all likely plant configurations. This is usually done by comparing the cut-sets produced by the two PSA models for the base case (all equipment available) and for cases with particular components removed from service. The more changes that have been made to the LPSA, the more extensive the validation process will need to be.

Risk monitor operation

The user of a risk monitor is limited to making changes to the plant configuration – that is, specifying the mode of operation of the plant, identifying which trains of systems are operating and which are on standby, identifying which components have been removed from service for maintenance or test, identifying whether the cross-connections between trains of safety systems are open or closed, etc. Good practice is to make the required inputs as soon as is convenient after the start of the maintenance activity so that the risk monitor follows changes to the plant in real time.

The precise outputs from the risk monitor depend on the software used and this typically includes quantitative risk information and qualitative safety status information.

The quantitative risk information includes: the point-in-time risk (CDF/ LERF); the risk profile that indicates how this has changed as a function of time due to changes in the plant configuration; a calculation of the allowed configuration time (ACT) – that is, the time that the plant can continue in the current configuration; and the cumulative risk as a function of time, which may be tracked and compared to a target. In addition, there is usually a means of evaluating the risk from proposed maintenance activities (what-if? calculations)

and future maintenance schedules. The importance of operating equipment and the quantitative reduction in risk that would be obtained by restoring equipment to service is also calculated.

The qualitative safety status information is typically in the form of safety system and safety function status. This provides a comparison of the plant configuration against deterministic criteria that relate to the level of redundancy, diversity and defence in depth of the safety systems. The coloured displays indicate when they are fully available/slightly degraded/degraded/not available. In practice, the definitions of the qualitative criteria used are deterministic and so, in many cases, there is not a direct correlation between the level of risk indicated by the calculation of the CDF/LERF and the qualitative status information.

Operational safety criteria (OSC)

When risk monitors are used on-line, it is usually the case that OSCs are defined that distinguish between the regions of low/moderate/high/ unacceptable risk where the actions that need to be carried out by the plant staff are different. In general, four regions of risk are usually defined and presented in a coloured display as follows:

- Unacceptable risk (red) which would normally only be entered when plant failure are identified. Planned maintenance is not allowed and immediate action is required to reduce the risk. A reactor shutdown may be required if this arises during power operation.
- High risk (orange) where severe time restrictions are imposed on the ongoing maintenance activities and compensatory measures may need to be introduced.
- Moderate risk (yellow) where there are time restrictions on the ongoing maintenance activities.
- Low risk (green) where there are no restrictions.

The OSCs can be defined either as absolute risk levels or as multipliers on the baseline (all equipment available) risk. The most common way of doing this is in terms of absolute risk levels. Although there are difficulties in justifying the numerical values used, this will provide a common basis for ensuring that all nuclear power plants are being operated to the same standard.

For the plants that defined the OSCs in terms of absolute risk levels, there is a broad consensus on how this needs to done. For full power operation, the boundary between the low and moderate risk bands is set at about the level of the average risk calculated in the LPSA. The reason for this is that, because one of the aims is to operate the plant in such a way that the actual risk averaged over the year is lower than the average risk calculated in the LPSA, the operators need to know when this level of risk is being exceeded. The boundary between the high and unacceptable risk bands is set at 10^{-3} per year for CDF and 10^{-4} per year for LERF. The boundary between the moderate and high risk bands is set at an intermediate level. However, it needs to be noted that the OSCs used will depend on the scope of the PSA used in the risk monitor and different criteria will need to be defined for use during the plant shutdown modes.

Allowed configuration time (ACT)

When risk monitors are used on-line, the ACT is usually calculated and displayed for the current plant configuration. The way that this is done is to control the overall (integrated) risk from each plant configuration above the low risk band such that the contribution that they make to the core damage/large early release probability is less than $10^{-6}/10^{-7}$ respectively.

Risk monitors also present information on when the configuration was entered and the time remaining. This is done for each new configuration as it is entered. In monitoring the ACT, the plant operators need to be aware of components that have remained out of service from the previous plant configuration and have already made a contribution to the core damage/ large early release probability. There is a need to define best practice in this aspect of the calculation and monitoring of ACTs.

Costs and benefits of risk monitors

The cost of implementing a risk monitor includes the purchase or development of the software to be used, and the cost of carrying out the conversion and enhancements of the LPSA model for use in the risk monitor application. These costs are well known from many successful risk monitor developments in the NEA member countries.

The primary benefit perceived by plant operators that have installed a risk monitor is that it is the most cost effective way of addressing risk issues related to operational safety requirements. In particular, the use of a risk monitor will:

- allow nuclear power plant operators in some of the NEA member countries to carry out more maintenance when the reactor is at power so that there will be a need for fewer, shorter periods of shutdown;
- provide a means of controlling the plant configurations thus ensuring that the overall risk from the plant will be lower which will give a hidden benefit;
- provide a basis for seeking exemptions from over-restrictive technical specifications and for extensions to the allowed outage times given in the technical specifications;
- provide risk information in a form that is readily understandable and can be used to demonstrate the level of safety of the plant;
- make it easier to address the US NRC maintenance rule which requires plants to assess the risk prior to entering a planned maintenance configuration and immediately after entering a non-voluntary configuration for all the modes of operation of the plant; and
- provide a basis for a wide range of risk-informed applications.

Since the costs of plant outages and maintenance are high, the benefits of the risk monitor are likely to be much greater than the costs incurred.

Issues and limitations related to the use of risk monitors

The PSA model used in the risk monitor will have the same limitations as those of the LPSA on which it is based. This could include limitations in the level of PSA carried out, the range of initiating events/hazards included and the modes of operation of the plant modelled. The risk monitor will only provide valid risk information and insights within the limits of the PSA that has been carried out. The emerging standard is for the risk monitor to be based on a full scope PSA that includes all initiating events and hazards, addresses both CDF and LERF and covers both full power operation and all the low power and shutdown modes.

There may be limitations in the risk monitor software used in that it may only provide a limited range of functions (none of the codes currently provide

the full range of functions that could be used). If the approach used is based on a pre-solved solution, this may lead to the risk being underestimated for some plant configurations. The need for a rapid solution has to be balanced against the accuracy of the risk estimate required.

There may be limitations in the scope and the detail of the conversion process from the LPSA to the risk monitor. Although the conversion process is well understood and there are many examples of how this has been accomplished successfully, care needs to be exercised to ensure that the extent and detail of the conversion carried out is appropriate to the potential uses of the particular risk monitor. The validity of the results obtained from the LPSA and risk monitor models is determined by the extent and documentation of the validation process carried out.

Uncertainties in the numerical results for CDF and LERF are not addressed explicitly by the risk monitor. The reason is that this facility has not been requested by any of the users of the risk monitor software codes. Hence, the uncertainties cannot be taken into account in the decision-making process.

However, it needs to be recognised that all the plants using a risk monitor have followed an integrated decision-making process. This combines the risk information and insights produced by the risk monitor with the deterministic requirements given in the plant technical specifications in reaching a decision. In doing this, the detrimental effect of many of the above limitations is minimised.

Concluding remarks

The following conclusion can be drawn regarding the state of the art in the development and use of risk monitor s at nuclear power plants:

- risk monitor s are the most influential development in PSA in recent years since they provide the ability to use the PSA on-line enabling the users to track and control the risk arising from changes in the plant configuration and environmental factors in real time.

- There are a large number of nuclear power plants throughout the world that are successfully using risk monitors. Hence, the development and use of risk monitors is a mature application of PSA.

- The perception of many nuclear power plant operators is that the use of a risk monitor is the most cost effective way of addressing risk in the safety management of the plant.

- There are a number of high quality risk monitor software packages commercially available or in use in the NEA member countries and others are being developed. They all provide a wide range of functions.

- The LPSA is not directly useable in a risk monitor and changes need to be made to remove simplifications made and to improve the models used. There is a large body of experience in converting a LPSA for use in a risk monitor application and carrying out the subsequent validation of this model.

- There is broad agreement on the way that the operational safety criteria used to distinguish between the regions of low/moderate/high/ unacceptable risk are defined and on how the allowed configuration Time should be calculated. The costs of implementing a risk monitor are likely to be very low compared to the benefits obtained.

- The issues and limitations related to the use of risk monitor s are well understood and accounted for by using the risk information it provides as one of the inputs into an integrated decision-making process.

- Some regulators are strong supporters of the use of risk monitors and are active users themselves, whereas others take a more neutral stance.

References

[1] *Risk Monitors: A Report on the State of the Art in their Development and Use*; IAEA-TECDOC; to be published jointly by IAEA and NEA in 2005. This report will also be available on the NEA website.

[2] Proceedings of the Workshop on Risk Monitor Developments; Madrid; to be published in 2005.

[3] *Living Probabilistic Safety Assessment (LPSA)*; IAEA TECDOC Series No. 1106; September 1999.

ALSO AVAILABLE

NEA Publications of General Interest

NEA News
ISSN 1605-9581 2005 subscription: € 49 US$ 56 £ 31 ¥ 6 600

Nuclear Safety and Regulation

Debris Impact on Emergency Coolant Recirculation (2004)
Workshop Proceedings, Albuquerque, NM, 25-27 February 2004
ISBN 92-64-000666-4 Price: € 90 US$ 113 £ 62 ¥ 11 500

Advanced Nuclear Reactor Safety Issues and Research Needs (2002)
Workshop Proceedings, Paris, France, 18-20 February 2002
ISBN 92-64-19781-8 Price: € 75 US$ 65 £ 46 ¥ 8 700

Collective Statement Concerning Nuclear Safety Research *Free: paper or web.*
Capabilities and Expertise in Support of Efficient and Effective Regulation of Nuclear Power Plants (2004) – ISBN 92-64-02169-8
Good Practice and Closer Criteria (2003) – ISBN 92-64-02149-3

Nuclear Regulatory Review of Licence Self-assessment (LSA) (2003)
ISBN 92-64-02132-9 *Free: paper or web.*

Regulator and Industry Co-operation on Nuclear Safety Research (2003)
Challenges and Opportunities
ISBN 92-64-02126-4 *Free: paper or web.*

Regulatory Challenges of Decommissioning Nuclear Reactors (The) (2003)
ISBN 92-64-02120-5 *Free: paper or web.*

CSNI Technical Opinion Papers *Free: paper or web.*
No. 1: Fire Probabilistic Safety Assessment for Nuclear Power Plants (2202)
No. 2: Seismic Probabilistic Safety Assessment for Nuclear Facilities (2202)
ISBN 92-64-18490-2

No. 3: Recurring Events (2003) – ISBN 92-64-02155-8

No. 4: Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants (2004) – ISBN 92-64-02157-4

No. 5: Managing and Regulating Organisational Change in Nuclear Installations (2004)
ISBN 92-64-02069-1

No. 6: PSA-based Event Analysis (2004) – ISBN 92-64-02091-8

Order form on reverse side.

ORDER FORM

OECD Nuclear Energy Agency, 12 boulevard des Iles
F-92130 Issy-les-Moulineaux, France
Tel. 33 (0)1 45 24 10 15, Fax 33 (0)1 45 24 11 10

E-mail: nea@nea.fr**, Internet: http://www.nea.fr**

Qty	Title	ISBN	Price	Amount
		Total		

θ Payment enclosed (cheque or money order payable to OECD Publications).

Charge my credit card θ VISA θ Mastercard θ American Express

(Prices include postage and handling fees).

Card No.	Expiration date	Signature
Name		
Address	Country	
Telephone	Fax	
E-mail		

OECD PUBLICATIONS, 2 rue André-Pascal, 75775 PARIS CEDEX 16
Printed in France.