Nuclear power plants: Using PSA to enhance operational safety

Probabilistic safety assessments are serving multiple needs

by L. Lederman and B. Tomic

Developed as a logical extension of the old engineering discipline of reliability analysis, probabilistic safety assessment (PSA) was introduced in the commercial nuclear power field in the mid-1970s. To date, more than 70 PSAs have been carried out worldwide for nuclear power plants. The studies provide safety insights that could not have been obtained by other means. In most countries with nuclear power programmes, PSA has become a standard tool for safety evaluations.

Briefly stated, PSA is a systematic method of modelling a plant's response to a set of initiating events that could threaten its safe operation. To develop the necessary models, detailed information regarding the plant's design and operation is needed. Basic models (such as fault or event trees) are developed to identify the success and failure paths. In analysing these models, a number of factors are taken into account, including the random failures of components, failures arising from a common cause, human errors, and test and operational strategies.

Some PSAs have been initiated by electric power utilities in response to regulatory concerns or to demonstrate low public risks associated with nuclear power plant operations (e.g., at the Zion nuclear plant in the United States, and the Sizewell plant in the United Kingdom). Other PSAs have been sponsored by regulatory bodies to promote and develop the use of the techniques. Moreover, as the methodology has matured, PSA results have been increasingly used for improving the operational safety of nuclear plants.

Involvement of national utilities

Experience with PSAs indicates that the utility's attitude towards the study, moreso than actual costs, determines the study's quality and the usefulness of results. In this context, it is important that the utility, in particular operational personnel, is involved from the early stages in the development of the plant model. This helps to make sure that realistic considerations are used. Such considerations include the completeness of the accident-initiating events considered, and their grouping; the plant response and the interactions among systems, the success criteria used for front-line systems, test and maintenance policies; operational procedures; and operator actions.

Plant-specific studies should make maximum use of all information available at the site, including data from past operating experience. Most important, however, is the commitment of plant and utility management to taking appropriate action involving design or operational changes indicated by the PSA.

In November 1988, the US Nuclear Regulatory Commission requested utilities to perform "individual plant examinations" to identify vulnerabilities to severe accidents based on a probabilistic approach. This NRC action promotes a more vigorous application of PSA and, to the maximum extent possible, encourages the commitment of the utility.

In some other countries, including Spain and Sweden, utilities have been requested to perform safety evaluations using PSA. In France, Electricité de France is about to finish a PSA study fully based on plant-specific information and data. It is going to be representative for a number of identical nuclear power plants.

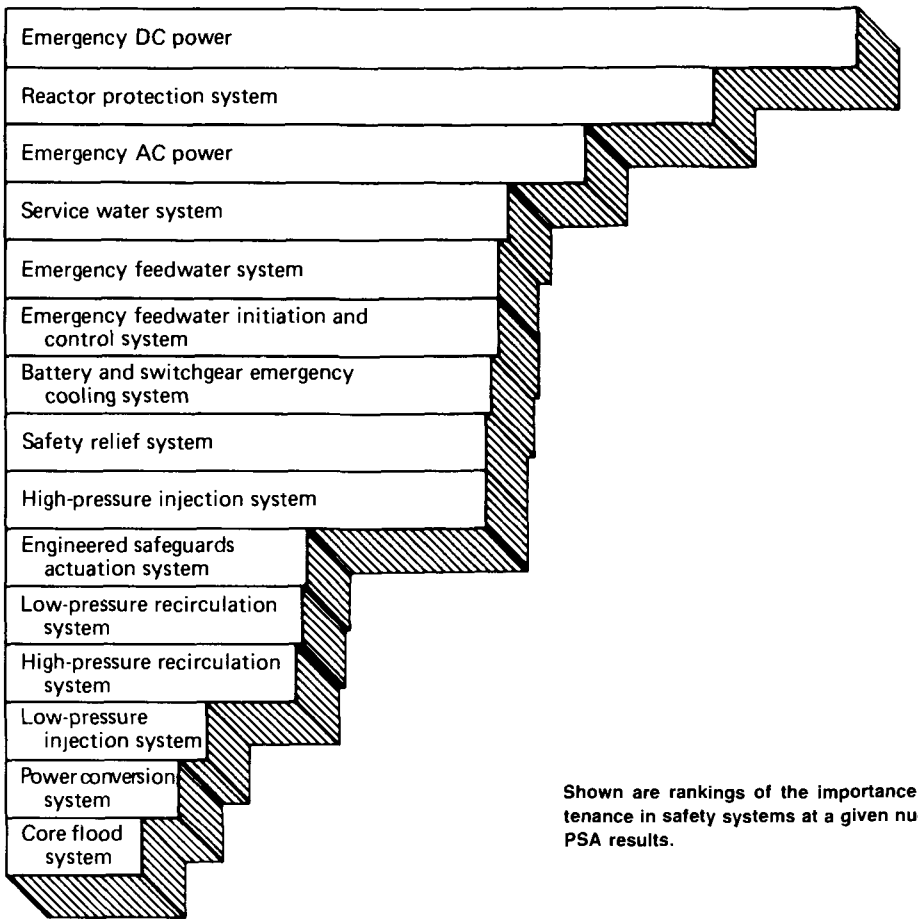
The "living" PSA

The nature of PSAs — namely the detailed modelling of systems and the representation of accident sequences in terms of basic component failures and human actions — sometimes makes it difficult for those not involved in the original study to fully understand and benefit from its results. It is not unusual for PSA reports to exceed 10 thick volumes. Indeed, some recent studies contain more than 10 000 pages of appendices with detailed models of plant systems.

Once the results are generated, the PSA needs to be continually updated and the results put into a form that allows for easy interrogation and retrieval. In this context, the concept of a "living PSA" has emerged and is gaining increasing attention.

Significant developments in the field of information technology, notably in the computing power of personal computers, have helped to address some of these needs. Software for personal computers that facilitates the

Messrs Lederman and Tomic are staff members in the IAEA Division of Nuclear Safety.



Shown are rankings of the importance of corrective maintenance in safety systems at a given nuclear plant based on PSA results.

selective interrogation of PSA results and the updating of models and data are being developed. (One type of software is briefly described later in this article.)

Such developments have enabled a better use of a wide range of PSA results. They have also helped to avoid viewing "bottom line" results — such as the frequency of a complete core meltdown — as the main insights derivable from a PSA. In fact, PSA results provide a wide range of benefits that allows plant management to more effectively focus and prioritize the use of available resources. *(See accompanying figure.)*

Practical applications of PSA results

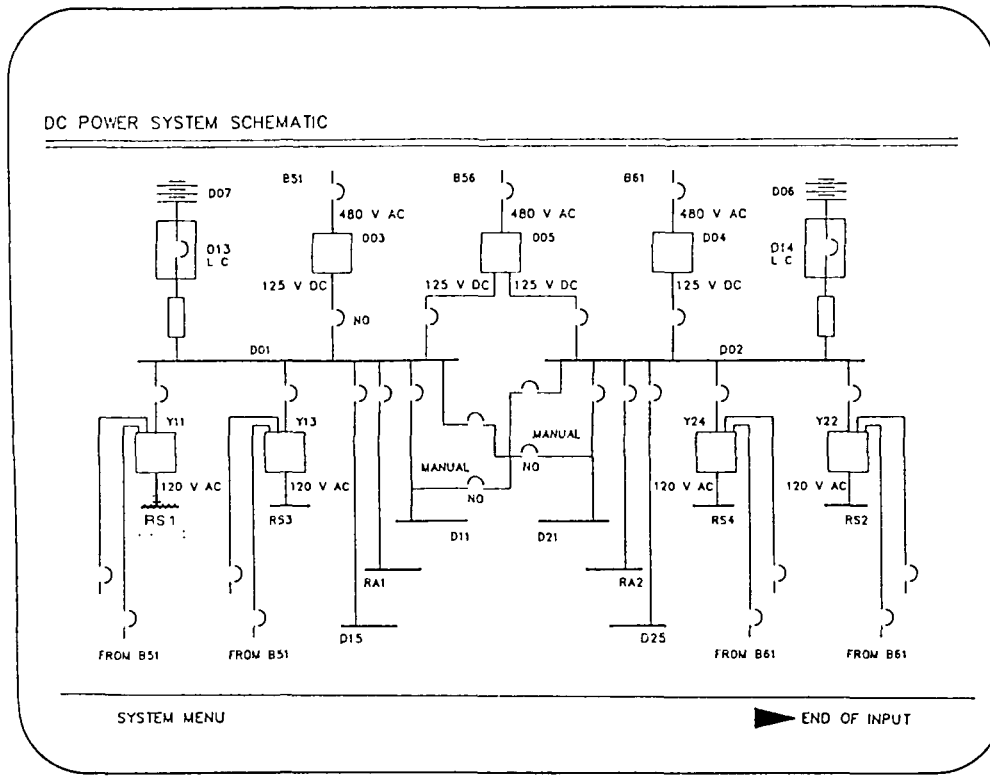
In a wide perspective, the current uses of PSA fall into two categories: plant backfittings; and operational management (including operational policy, assessment of plant status, and operator training).

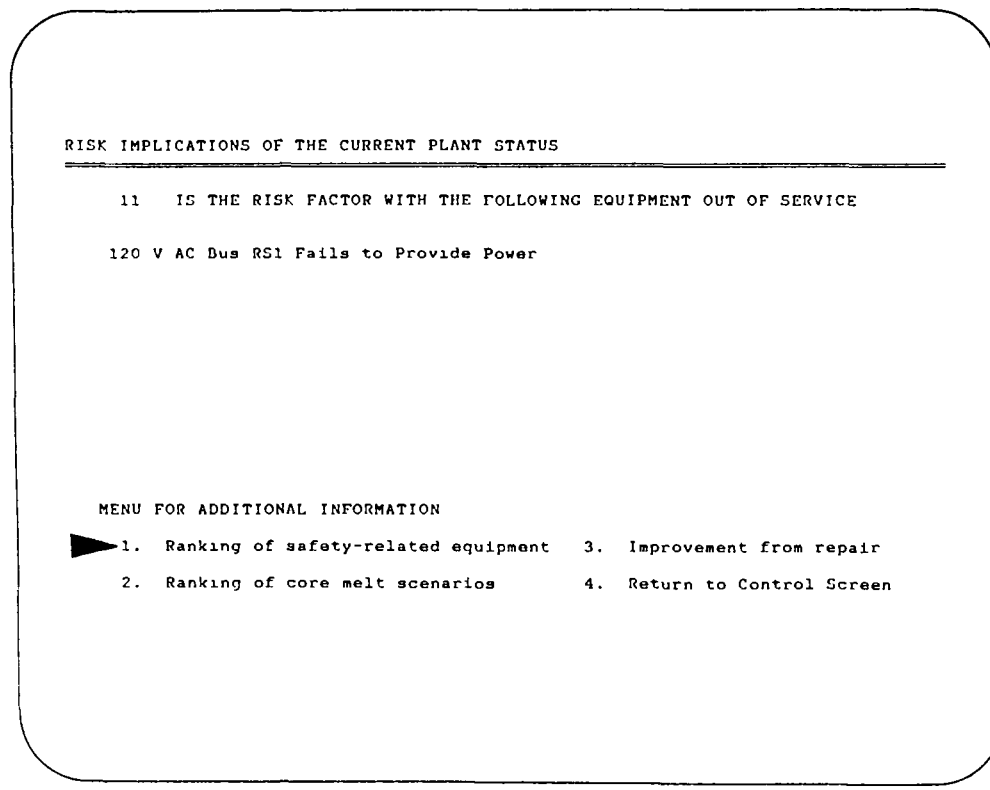
Plant backfittings. Results of PSA studies usually indicate areas of plant design where improvements would result in the greatest benefit. These results are often used by the utility for planning design modifications, and for evaluation of the safety significance of a modification proposed or required by the regulatory body.

A recent study in the United States by the Electric Power Research Institute (EPRI) reports on practical applications of 26 PSAs cited by 10 US utilities.* Following are some examples of the benefits that utilities have derived from PSAs performed for specific nuclear power plants:

- At Millstone-1 in Connecticut, a regulatory requirement for diverse level instrumentation was shown to be of no safety significance and an alternative modification was accepted at a savings of about US $250 000. In another instance, the plant was able to obtain an exemption regarding the qualification of a number of motor-operated valves. Savings of US $2–3 million were realized, and occupational radiation exposures that the work would have entailed, were avoided.
- At the Yankee plant in Massachusetts, exemption was obtained from regulatory requirements on a number of

* "The Practical Application of Probabilistic Risk Assessment", EPRI, NP-5664 (March 1988).





Software that can be used to apply PSA results to the management of safety at nuclear plants has been developed for personal computers. Shown here are reproductions of two computer screens for the PRISIM software. At the top is a schematic of the plant's *direct-current* power system; below is a message concerning the risk implications for a situation with the 120 V AC bus out of service. A computer screen menu shows headings for additional information. (The software is available in English only.)

containment penetrations, resulting in savings of US $16 million. At the same plant, a significant design deficiency was identified in the power supplies to cooling-water valves of the diesel generator.

● At the Big Rock Point plant in Michigan, the successful resolution of a long list of regulatory issues amounted to total savings estimated between US $20–40 million. The utility credits the PSA with ensuring the plant's current operation.

● At the Catawbe plant in South Carolina, a potential system failure in the event of station blackout was identified and resolved.

Operational management. Countries operating nuclear power plants have set operational limits and conditions that are often referred to as technical specifications for nuclear plant operations.

Technical specifications are in most cases based on engineering judgement or common sense and may not be optimized from the safety standpoint. Some requirements could be burdensome for operating personnel and could lead to unnecessary radiation exposures. In that respect, PSA results can be used to systematically determine technical specification requirements. Such results are most useful in justifying the technical basis for certain conditions of operation, in particular, surveillance test intervals and allowed outage times.

Surveillance tests are done to detect potential failures, and, therefore, serve as a way of controlling risks. If done too frequently, however, the tests themselves can increase risks by, for example, causing plant transients or taking some components temporarily out of service. From the standpoint of operations, a long interval between surveillance tests is favoured, but that may not be adequate for assuring the plant's overall safety. Similar competing considerations apply to the duration of allowed outages.

Considering these facts, PSA has been found useful for analysing the technical specifications for surveillance tests and outage times, with a view toward improved management of the plant's overall safety while allowing for more operational flexibility. The evaluation of technical specifications based on PSA methods is being done in the United States and in Nordic countries, among others.

Plant status monitoring. Until recently the large body of information contained in a PSA has been used essentially in a static and limited manner. One reason for this is that even small changes that are necessary to reflect actual system configurations during operation entail substantial recalculations.

In a meeting convened by the IAEA in 1987, efforts to use PSA information for day-to-day operational safety management on personal computers were reviewed.* A software package was presented for use with personal computers (called PRISIM) that is capable of interrogating results of a completed PSA to assist plant personnel and regulatory inspectors. Plant operators can use the software to determine safety implications if, for example, specific combinations of equipment were to be placed out of service for testing or maintenance at a particular time. Plant inspectors can quickly access PSA results in the field to make decisions about, for example, returning out-of-service equipment to service or ensuring that other equipment is operable; and about the scheduling of inspection efforts based on trends in failures of components and systems, and their importance to operational safety. *(See figure, page 41.)*

Operator training. Insights from PSA are of great value for training nuclear plant operators, particularly with respect to severe accidents. The multiplicity of potential accident scenarios developed in PSAs contain valuable information on the plant response to a wide range of observed and anticipated accident initiators. These sequences combine multiple system failures and human errors and are by their very nature rare events which may lead to core damage. Therefore, nuclear plant operators must be aware of these situations. In-

IAEA activities in the field of PSA

Function	Activity
Exchange of scientific information	• Technical committee meetings, symposia, seminars, conferences, and associated publications
Development of standards	• Guidelines for conducting PSA for nuclear power plants • Specific guidelines on human error probabilities • Specific guidelines on external hazards • Specific guidelines on common cause failures • Specific guidelines on PSA computer codes • Specific guidelines on reliability data collection and analysis • Specific guidelines on procedures for peer reviews • Probabilistic safety criteria
Training	• Training courses for PSA managers • Training courses for PSA analysts • Workshops on specific PSA issues
Technical co-operation and assistance	• Missions to Member States to assist in planning and implementing PSA programmes
Promotion of research and development	• Co-ordinated research programme on data collection and analysis for PSA • Co-ordinated research programme on benchmark studies on accident sequences of PSA
Operations and services	• International peer review teams to review results of PSAs in Member States • Evaluation of operational experience at nuclear power plants using PSA insights • Nuclear power plant operational safety management using PSA results (PSAPACK)

* For a report on the meeting, see *Improving Operational Safety Management through PSA on Personal Computers*, IAEA-TECDOC-480 (1988). See also "PRISIM — A Computer Program that Enhances Operational Safety", by Fussel, J.B., NUREG/CR-5021, Vol. 2 (March 1988).

volving operators in the development of PSA is a natural means of training.

PSA insights are also valuable in the development of emergency operating procedures and are useful for operator training on simulators. At an IAEA technical committee meeting, Electricité de France reported its use of two PSA-based accident scenarios for operator training on full-scope simulators.*

IAEA activities

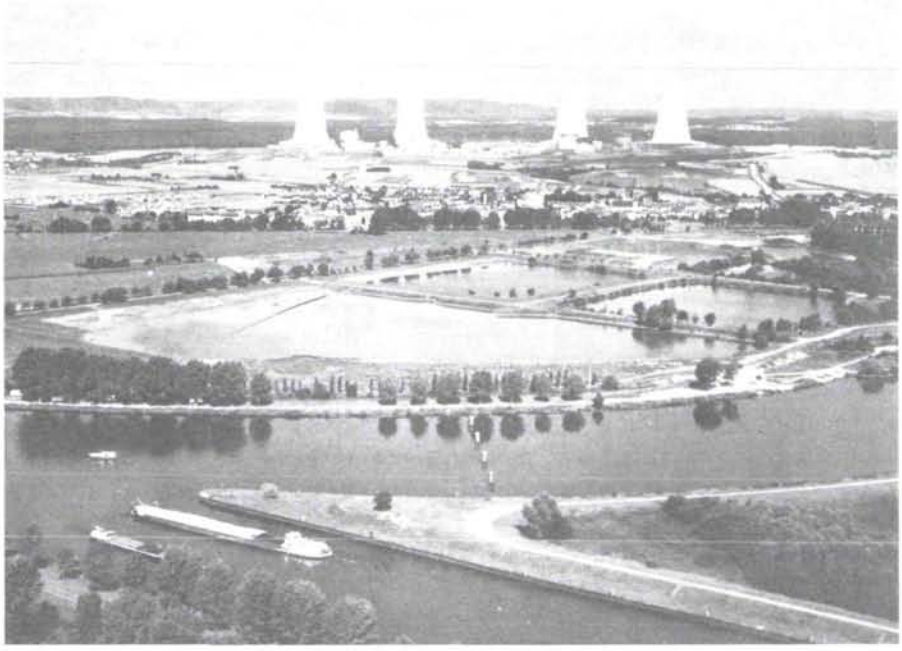
Recent IAEA activities in the field of PSA have been organized in accordance with high-priority recommendations that were formulated from insights of the Chernobyl nuclear plant accident in 1986. The PSA programme has three distinct elements: (1) promoting, assisting, and facilitating the use of PSA by reviewing the techniques developed in Member States for the use of PSA; (2) assisting in the formulation of guidelines for PSA use; and (3) helping Member States to apply such PSA guidelines to enhance safety in all nuclear power plant operating modes. *(See accompanying table.)*

The work on PSA guidelines aims at the establishment of a consistent framework for the conduct of a PSA and for reporting the results. These guidelines will be published in forthcoming IAEA Safety Series documents. Special attention is given to the documentation of the analysis and to the display and interpretation of PSA results. The work is directed at alleviating problems connected with the complexity and diversity of PSA reports.

In response to the need for provision of quick and easy access to PSA results, the IAEA has developed a software package, called PSAPACK, for performing a PSA. Work has now started on extending the computer program to facilitate the use of PSA results in support of nuclear plant safety management. PSAPACK is intended for use on personal computers and has been widely distributed by the IAEA.

Given the value of PSA for practical applications in the overall management and assessment of nuclear plant safety, it holds considerable potential in support of other safety activities of the IAEA. These will include operational safety reviews of nuclear plants; the development of numerical indicators concerning plant performance and trends; and the evaluation of the safety significance of abnormal occurrences at nuclear power plants.

* For a report on the meeting, see *Experience with Simulator Training for Emergency Conditions*, IAEA-TECDOC-443 (1987).



Cattenom nuclear power station, France. (Credit: Framatome)