Probabilistic safety assessment: Growing interest

PSA has matured into a useful tool for reactor safety

by Luis Lederman

Probabilistic methodology in reliability and safety evaluation today is attracting considerable attention in nuclear power and other fields. Yet it is far from being a new idea. It can be traced back to, at least, the early 1940s when quantitative probabilistic safety requirements were first proposed for the aeronautics industry. The probabilistic term then was that an airplane accident would not happen more than once per 100 000 hours of flight time.

In 1942, when the high failure record of the German V-2 rocket programme was studied, the concept of dependency between parts of a system was introduced as a step ahead of the prevailing belief that a system was only as good as its weakest part. That started a logical and integrated systems analysis approach. During the following two decades, initial concepts were refined and expanded – including the development of statistical models to analyse component failures and reliability theory.

In 1960 further development was achieved with the use of logical analysis in connection with the Apollo programme of the US National Aeronautics and Space Agency (NASA). An important tool called "failure mode effect and criticality analysis" was then introduced. In 1962 the Bell Telephone Laboratories in the USA used the fault-tree technique in a study for the US Air Force on the reliability of launching and controlling Minuteman missiles. In the nuclear power field, a limit line for accidental iodine releases was first proposed in terms of the probabilities of occurrence by F.R. Farmer of the United Kingdom in 1967.

The pioneering report in the application of probabilistic methodology to nuclear reactor safety was WASH-1400, generally known as the Reactor Safety Study. Published in 1975, the study analysed two light-water reactors (one pressurized-water reactor and one boiling-water reactor) in terms of the probabilities and consequences of potential accidents.

The study followed by some 18 years the first attempt to analyse consequences of possible catastrophic nuclear plant accidents – a study reported as WASH-740. This study envisaged progressive stages of nuclear accidents in a nuclear power plant based on subjective probabilities and calculated off-site consequences. The results had no practical use, however, because of the lack of information available about plant design data and the very limited knowledge of methods needed for such an analysis.

Such was not the case with WASH-1400, which did have an impact. It aimed at responding to three basic questions formulated in a probabilistic safety assessment:

- What can go wrong?
- What is the frequency of occurrence?
- What are the consequences?

WASH-1400 applied the newly developed methods of reliability analysis, the data available from the nuclear and non-nuclear industries, statistical models and the existing knowledge about the degraded core phenomenology, release of radionuclides, and off-site consequences. Human failures, common cause failures, and propagation of uncertainties also were treated, despite the limited understanding that existed about them.

Unfortunately, the study's complexity and difficulties in reporting results combined to downplay its potential for evaluating reactor safety. In fact, the report was misinterpreted, primarily as a result of an analysis called the Lewis Report that was prepared by a review group formed by the US Nuclear Regulatory Commission (NRC). The consequence was that probabilistic techniques became the subject of much controversy.

The Three-Mile Island (TMI) accident in 1979 changed the picture dramatically. Post-accident study groups, notably the Kemeny Commission, urged greater emphasis on probabilistic techniques. In its report, the Kemeny Commission recommended that "continuing in-depth studies should be initiated on the probabilities and consequences (on-site and off-site) of nuclear power plant accidents, including the consequences of meltdown" as part of the formal safety assurance programme.

Moreover, when it was found that WASH-1400 had foreseen sequences similar to those leading to the TMI accident, the use of probabilistic methodology in nuclear safety gained additional momentum.

Mr Lederman is a staff member in the Agency's Division of Nuclear Safety.

PRA studies done to date

Ten years after the publication of WASH-1400 – and six years after TMI – the probabilistic technique today is a maturing and useful tool to evaluate reactor safety. Acronyms such as PRA (probabilistic risk assessment), PSA (probabilistic safety assessment), RSSMAP (reactor safety study methodology application), IREP (interim reliability evaluation programme), and NREP (national reliability evaluation programme) have become part of the everyday jargon in the nuclear safety field.

Many PSA studies already have been done and more are in progress in several countries. (The IAEA has defined PSA as the appropriate application of probabilistic risk assessment methods to nuclear safety decisions.) The accompanying table reports results from some of them.

Some studies have been sponsored by governmental organizations – as in the cases of WASH-1400 in the USA and the German Risk Study in the Federal Republic of Germany. Many others were conducted entirely by the industry or as joint ventures.

A class of these studies was motivated by the need to extend the scope and value of the Reactor Safety Study leading to the RSSMAP. Others were carried out as plant-specific investigations (e.g., those under the IREP and NREP). Industry-sponsored studies also have been initiated by utilities in response to backfitting requirements, as a tool for training operating personnel, and/or to evaluate public risks from operating facilities near heavily populated areas. In the USA, the Big Rock Point study is an example of the former goal, whereas the Zion and Indian Point studies are examples of the latter.

Although conducting a PSA in most countries is not an integral part of the licensing process, the completed studies are normally submitted to the regulatory authorities for review and the insights obtained are being used in supporting safety decisions. In 1982, the Limerick study was the first one sponsored by industry in the USA that was conducted in response to a specific licensing requirement. More recently a PRA was submitted to the US NRC as part of the General Electric Standard Plant Safety Analysis Report (GESSAR-II).

Emphasis on practical results

Current trends in PSA have been noted at several recent gatherings. At the international meeting of the American Nuclear Society (ANS) and the European Nuclear Society (ENS) on Probabilistic Safety Methods and Application (held in San Francisco this past March),

PRA study results – core-melt frequencies

Plant	Rating (MWe)	Type, NSS supplier	Programme date	Core-melt probability per year
Arkansas-1	836	PWR, B&W	IREP, 1981	5 X 10^{-5}
Biblis B	1240	PWR, KWU	DRS, 1978	4 X 10^{-5}*
Big Rock Point	71	BWR, GE	Utility, 1981	1 X 10^{-3}
Browns Ferry-1	1065	BWR, GE	IREP, 1981	2 X 10^{-4}
Calvert Cliffs-1	845	PWR, CE	RSSMAP, 1982	2 X 10^{-3}
Crystal River-3	797	PWR, B&W	IREP, 1980	4 X 10^{-4}
Grand Gulf-1	1250	BWR, GE	RSSMAP, 1981	4 X 10^{-5}
Indian Point-2	873	PWR, W	Utility, 1982	4 X 10^{-4}*
Indian Point-3	965	PWR, W	Utility, 1982	9 X 10^{-5}*
Limerick	1055	BWR, GE	Utility, 1982	3 X 10^{-5}*
Millstone-1	652	BWR, GE	IREP, 1982	3 X 10^{-4}
Millstone-3	1150	PWR, W	Utility, 1983	1 X 10^{-4}
Oconee-3	860	PWR, B&W	RSSMAP, 1980	8 X 10^{-5}
Peach Bottom-2	1065	BWR, GE	WASH-1400, 1975	3 X 10^{-5}*
Ringhals-2	800	PWR, W	SSPB, 1983	4 X 10^{-6}
Seabrook	1150	PWR, W	Utility, 1983	2 X 10^{-4}
Sequoyah-1	1148	PWR, W	RSSMAP, 1981	6 X 10^{-5}
Shoreham	819	BWR, GE	Utility, 1983	4 X 10^{-5}
Sizewell B	1200	PWR, W	CEGB, 1982	1 X 10^{-6}
Surry-1	788	PWR, W	WASH-1400, 1975	6 X 10^{-5}*
Yankee Rowe	175	PWR, W	Utility, 1982	2 X 10^{-6}
Zion	1040	PWR, W	Utility, 1981	7 X 10^{-5}*

Note: *Table includes external event contribution where appropriate. Comparisons of values listed should be made with extreme caution. Different models, assumptions and degrees of sophistication were employed.*

* Values which are asterisked represent median values; otherwise point estimates are listed.

Source: *Risk Analysis,* Vol.4 (December 1984).

considerable emphasis was placed on practical applications and real benefits of PSA studies. Previous meetings in the field had focused largely on methodology. Highlights from some of the 190 papers presented follow.

Safety goals

Safety goal implementation has been reviewed in the USA and in Europe. Since 1983, the evaluation effort has been conducted by the US NRC, and a policy statement concludes that safety goals can be used in the regulatory process to augment the traditional safety review methods. The statement cautions, however, that they should not be used within a regulatory framework of strict acceptance or non-acceptance criteria. In Europe, the first results of a task force organized in 1983 to review the issue are even more cautious. Safety goals related to risk analysis may give guidance in the rule-making process, although it is not clear at this time how implementation will be possible.

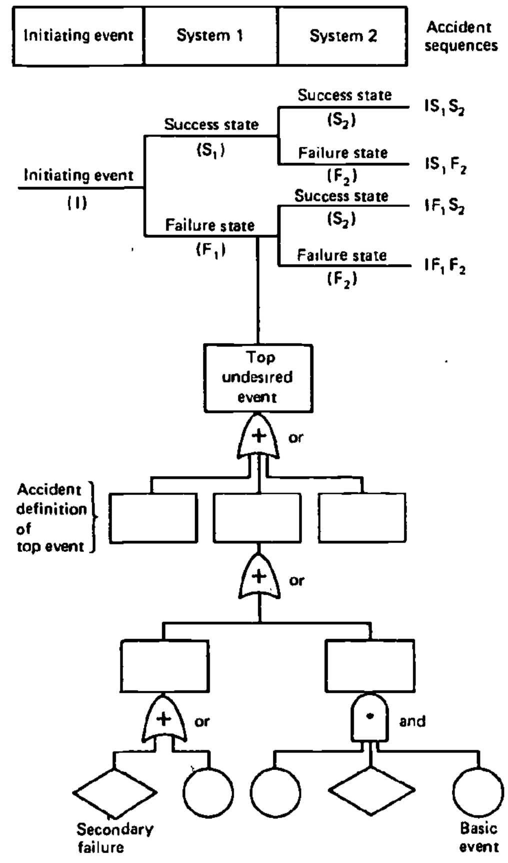
Data bases improving

Several papers at the ANS/ENS meeting reviewed the key US data bases relevant to PSA studies and reported a very encouraging situation, especially so when compared with the "data weak" condition of the industry at the time of WASH-1400.

The data base (Std.500 1984) of the Institute of Electrical and Electronic Engineers (IEEE) was shown to have gone a long way towards becoming a standard for nuclear plant risk and reliability analysis. Significant re-scoping and re-structuring of the Nuclear Plant Reliability Data System (NPRDS) operated by the Institute of Nuclear Power Operations (INPO) since 1983 indicates that it may well become a significant data source in the future. It will include data from all operating nuclear power plants in a consistent and comprehensive fashion, as well as provide on-line access for data entry and retrieval.

The European Reliability Data Bank, a centralized system collecting and organizing information related to the operation of light-water reactors, also was reviewed. Emphasis was given to the increasing role that artificial intelligence techniques – such as natural language and expert system and fuzzy logic – may play in improving future capabilities of the four data banks constituting the system: These are the component event data bank, operating unit status report, abnormal occurrences reporting system, and the reliability parameters data bank.

The data collection and analysis programme on human error – jointly undertaken since 1982 by Electricité de France and INPO – was described. Major issues reported included cognitive factors in human failures, times at which failures occur, place of failures, time between failure occurrence and detection, and characteristics of tasks leading to failures.



An example showing event tree branching and levels of fault tree development.

Applications: positive reports

Extremely positive reports on applications of PSA by the industry and regulatory bodies were presented. Utilities reported their established capabilities to perform, use, and maintain PSA models for their plants. Uses of PSA in safety management, and as a decision tool in engineering and operational areas, are seen to be part of an "integrated living schedule" of plant modifications and budget allocation.

Specific regulatory applications reported included a probabilistic analysis of pressurized thermal shock that is helping the US NRC and the industry to resolve this problem. In particular, the analysis helps identify important sequences leading to a through-the-wall crack and helps define operator and control actions.

PSA software, guides, and resources

Much has been accomplished in the area of PSA methodology development since WASH-1400 was published. Weak areas identified during the Lewis Review have been pursued. These include human reliability analysis; identification and treatment of uncertainties due to parameters; modelling and completeness; and data collection and treatment necessary to support PSA studies.

In the area of computer codes, a large variety of codes are available for the quantitative evaluation of large fault trees and event trees, for aiding in the identification of common-cause failures, and to analyse propagation of uncertainties. Other codes have been or are being developed to handle the degraded core phenomenology, containment behaviour, and off-site consequences. Areas not contemplated in WASH-1400 also have been given much attention, in particular the fire hazards analysis and the treatment of external accident-initiating events. In the latter category, several studies have shown that seismic events dominate the risk.

The availability of PSA-related literature has exploded in the past years. Apart from detailed PSA reports that have been published describing the methodology and results obtained, many reports more sharply focused have been issued by regulatory bodies and national laboratories.

Various guidebooks have documented procedures for conducting a PSA. In the USA, the IREP guide was published in January 1983. In parallel to it, the US NRC, the Electric Power Research Institute (EPRI), the Institute of Electrical and Electronics Engineers (IEEE), and the American Nuclear Society (ANS) undertook a broader effort, issuing a *PRA Procedures Guide.* This is a compendium of recognized methods for conducting a PSA. It defines levels of PSA studies that now are widely referenced: *Level 1* includes systems analyses leading to core-melt frequency assessment. *Level 2* includes containment analyses leading to releases, and *Level 3* provides a full assessment of public risks by virtue of inclusion of off-site consequences.

Perspectives, potential

Current uses of PSA in reactor safety have served to unfold the enormous potential of these techniques, in particular to study technical issues in situations where the purely deterministic approach is insufficient. As more insights are gained from PSA studies, even more emphasis likely will be placed on PSA techniques by utilities and regulatory authorities alike.

Following are some special areas of PSA utilization: identification of systems and components important to safety; evaluation of technical specifications including limiting conditions of operation (LCO); backfitting, including cost/benefit analysis; training of operators, plant staff, and regulators; design evaluation, including common-cause failures and human errors; identification, evaluation, and ranking of safety issues; emergency preparedness planning; allocation of inspection activities; accident management; simulation of accident scenarios; test, maintenance, and repair policy; compliance with target values; and risk management.

Additionally, government and industry organizations today are conducting various research programmes to resolve problems encountered in the utilization of PSA. Among areas being addressed are the identification and treatment of uncertainties; the considerable degree of judgement in almost all aspects of human reliability evaluation; the disagreement about the frequency of occurrence of common cause failures and accepted means of analysis; the methodology developments needed for the analysis of systems interactions; the large uncertainties associated with the calculated risks from external initiators; and the characterization of source term uncertainties.

The development of general licensing criteria, in particular the controversial use of safety goals, is much influenced by political and psychological issues regarding the general level of acceptable risk. Fortunately, most PSA applications do not depend on the outcome of such ongoing discussions and, therefore, reactor safety can continue to benefit from them.

In summary, then, it should be stated that PSA is not a way to present existing knowledge in a probabilistic framework. Rather, it is a recognized and effectively used engineering investigation tool for reactor safety that provides safety-related insights not reached through any other means.

Agency activities in PSA

IAEA programmes in this field are focusing on three distinct aspects:

- The trend from estimates of overall risks to identification of dominant accident sequences to reliability analyses of systems important to safety
- Initiation of PSA programmes in many Member States
- PSA efforts on decision-making

In this context, an interregional programme was recently initiated with the objective of co-ordinating ongoing training activities and of establishing within the nuclear regulatory authorities of developing Member States teams capable of performing probabilistic safety assessments.

Other activities include:

- *Preparation of technical reports.* These are being done in the areas of PSA and operating experience; status and future prospects for the development of quantitative safety goals; identification of failure sequences sensitive to human failure; and PSA of engineered safety systems.

A document on PSA utilization and implementation for safety decisions under preparation is expected to fill an important gap in the field. Specifically, it will assist in the standardization of methods, applications, and interpretation of PSA results.

- *Research projects.* A co-ordinated research programme to develop risk criteria for the nuclear fuel cycle was started in 1982 with the participation of 17 countries.
- *Training and support.* IAEA is organizing a short course to meet the needs of managers planning to incorporate a PSA group into their activities. Already, a seven-week course for analysts is given once a year and is intended to provide guidance in conducting PSAs and correctly using the results. Also being implemented in Vienna for use by Member States are computer codes for PSA applications.