



GOVERNMENT OF INDIA

**PROBABILISTIC SAFETY ASSESSMENT
OF
NUCLEAR POWER PLANTS
A MONOGRAPH**

R. B. Solanki and Mahendra Prasad
Safety Analysis and Documentation Division



**ATOMIC ENERGY REGULATORY BOARD
NIYAMAK BHAVAN
ANUSHAKTINAGAR
MUMBAI-400 094
INDIA**

**PROBABILISTIC SAFETY ASSESSMENT
OF
NUCLEAR POWER PLANTS
A MONOGRAPH**

by
R. B. Solanki and Mahendra Prasad
Safety Analysis and Documentation Division

**Atomic Energy Regulatory Board
Mumbai-400 094
India**

November 2007

1. INTRODUCTION

This monograph on probabilistic safety assessment (PSA) is addressed to the wide community of professionals engaged in the nuclear industry and concerned with the safety issues of nuclear power plants (NPPs). While the monograph describes PSA of NPPs, the principles described in this monograph can be extended to other facilities like spent fuel storage, fuel reprocessing plants and non-nuclear facilities like chemical plants, refineries etc. as applicable. The methodology for risk assessment in chemical plants or refineries is generally known as quantitative risk analysis (QRA). The fundamental difference between NPP and chemical plant is that in NPPs the hazardous material (fuel and fission products) are contained at a single location (i.e. inside containment), whereas in a chemical plant and reprocessing plants, the hazardous material is present simultaneously at many places, like pipelines, reaction towers, storage tanks, etc. Also unlike PSA, QRA does not deal with levels; it uses an integrated approach combining all the levels.

The monograph covers the areas of broad interest in the field of PSA such as historical perspective, fundamentals of PSA, strengths and weaknesses of PSA, applications of PSA, role of PSA in the regulatory decision making and issues for advancement of PSA.

2. PSA-HISTORICAL PERSPECTIVE

PSA is a systematic and comprehensive methodology to evaluate risks associated with every life-cycle aspect of a complex engineered technological entity such as a facility, a spacecraft, or a nuclear power plant. PSA has emerged as an increasingly popular analytical tool in the last couple of decades. This section provides a brief history of the introduction and subsequent use of PSA in the aviation, aerospace and nuclear sectors.

2.1 Aviation and Aerospace Sectors

In the aviation, safety and risk are of paramount importance. The Boeing Company, in conjunction with Bell Laboratories, pioneered the use of fault tree analysis during the design of the Minuteman missile for the U. S. Air Force during the 1960s to prevent inadvertent launches. As the Boeing-747 would be the largest commercial jet in operation at the time of its introduction, the Boeing engineers felt that it would be important to look at the safety systems of the plane in a different manner than what was being done for the earlier aircraft designs. The fault tree analysis technique was used, which provided a deductive, systematic and holistic assessment of the airplane systems, and highlighted the critical faults.

Probabilistic analysis of aircraft gained popularity during the 1970s. A 1979 crash of a DC-10 at O'Hare International Airport led to re-assessment of aircraft safety. Eventually, in 1982, the U. S. Federal Aviation Agency recommended to use fault tree analysis for new aircraft designs for identifying single points of failure and reduce the chances of such failures to less than one-in-a-billion flight hours. However, considering the number of single failures in an aircraft, the actual rate for the whole aircraft is probably one-in-20-million flight hours or so, assuming proper maintenance. Without proper maintenance, the rate of failure could rise dramatically.

NASA began to use probabilistic risk assessment (PRA) methods in 1967, after the disastrous fire on Apollo 1. They relied on highly conservative measures and data and estimated failure probabilities for Apollo missions to be in the range of 0.1-0.8 per mission; a range that was significantly higher than the actual experience. This led to skepticism and distrust of PRA techniques. However, following the Challenger explosion in 1986, probabilistic risk assessment at NASA was revived, and the Columbia break-up in 2003 reiterated the need for such analyses. NASA used risk assessment and a combination of fault and event tree methods borrowed from the nuclear industry to model possible accident scenarios for the shuttle and international space station programs. One risk study performed by the US Air Force in 1983 calculated the chances of a space shuttle solid rocket booster failing during operation to be about 1 in 35, a number that was initially disputed by NASA management.

While initially, the use of risk assessment methods in the nuclear industry benefited significantly from the experience of the aerospace industry in the early 1970s, in the late 1980s, when the need for systematic safety assessment became more apparent, it was the aerospace industry that it turned to and started relying heavily on the experience of the nuclear industry in use of PRA.

2.2 Nuclear Sector

The U.S. Atomic Energy Commission pursued the philosophy of risk assessment based on 'maximum credible accident' throughout 1950s, following the '**Atoms for Peace**' program. Because the 'credible accidents' were covered by plant design, residual risk was estimated by studying the consequences of hypothetical 'incredible accidents'. An early study released in 1957 focused on the radioactive releases from a 200 MWe NPP operating 30 miles from a large population center. Successive design improvements were intended to reduce the probability of catastrophic release of radioactive inventory from the reactor core. Plans were also being drawn for reactors in the 1000 MWe range located close to population centers. All these developments would have impact on the consequences of the 'incredible accident'. The desire to quantify and evaluate the effects of the various improvements led to the introduction of 'PRA'.

The first full-scale application of PRA was undertaken in the reactor safety study (RSS) WASH-1400 published by U.S. nuclear regulatory commission (NRC) in 1975. The American physical society conducted an extensive review of the first draft of WASH-1400. It was concluded that the calculation methods of WASH-1400 were 'fairly unsatisfactory'. In 1977, a special review panel of external reactor safety experts led by Prof. Harold Lewis recognized the basic validity of the PRA methodology and expressed the appreciation for the pioneering effort put into RSS study. However, the panel discovered many deficiencies in RSS study in the treatment of the probabilities.

In January 1979 the NRC distanced itself from the results of the RSS study. In March 1979, Three Mile Island (TMI-2) suffered a severe core damage accident. The post accident analysis revealed that the accident sequence was infact, predicted by RSS study. Two influential independent analyses (the report of the president's commission on TMI-2 accident and the Rogovin report) credited the RSS study with identifying **the small break LOCA as a major threat to safety**, and recommended that greater use should be made of PRA in assessing the risk of NPPs. Shortly after this, new generation PRAs have been performed in which the deficiencies of the RSS study were removed. In 1986, the NRC started PRA study known as 'NUREG-1150', which was published in December 1990. Since then PRA has gained significant importance and is now increasingly being used for assessing safety of NPPs. To make the risk assessment technology and methods available to the industry, in November 1988, the NRC issued the Generic Letter 88-20, 'Individual Plant Examination for Severe Accident Vulnerabilities'. As a result, 74 PRAs with varying degrees of details, representing 106 US nuclear power plants were completed by 1992. Since then PRA has come to stay as an essential element in the overall safety assessment of not only NPPs but also all the nuclear facilities.

In India, Bhabha Atomic Research Centre (BARC) is carrying out PSA studies since eighties. Nuclear Power Corporation of India Limited (NPCIL) has developed dedicated PSA groups at headquarters and at different NPP sites. Other organisations of Department of Atomic Energy (DAE) like Indira Gandhi Centre for Atomic Research (IGCAR), Kalpakkam are also making significant progress in the PSA studies. Level 1 PSA with internal events are now available for all operating NPPs.

Many of these PSA studies needed refinement with regard to comprehensiveness and selection of initiating events (IEs), level of details, modeling approach, assumptions and evaluation of data. Computer packages used for analyses varied from in-house developed ones to internationally used ones (e.g. PSAPACK, Risk-spectrum etc.). Efforts are on for PSA studies with external events such as fire, seismic and flood. The overall progress of PSA status is very encouraging.

3. PSA-AN OVERVIEW

In this section, the definition of PSA, different levels of PSA and comparison of PSA with the deterministic approach are discussed.

3.1 What is PSA ?

PSA is a methodical and logical tool for deriving numerical estimates of risk from a nuclear power plant (or indeed any plant in general). PSA usually answers three basic questions: (i) What can go wrong with the entity under study ? (i.e. undesirable starting events) (ii) What and how severe are the potential detriments or consequences that the entity under study may be subjected to ? and (iii) How likely these undesirable consequences are to occur?

PSA differs from the traditional deterministic analyses in that it provides a methodical approach to identifying accident sequences that can result from a broad range of initiating events. It includes the systematic determination of accident frequencies and consequences, and aims as much as possible to be 'best-estimate' (i.e. unbiased estimate which has a minimum variance). How true this last statement is depends upon the amount, quality and type of information available for use in the PSA, and in many areas, due to lack of information, pessimistic assumptions have to be made. PSA provides important safety insights such as insights into plant design, performance and operation as well as environmental impact, and the identification of dominant risk contributors.

In practice PSA aims to achieve completeness in defining possible mishaps, deficiencies and plant vulnerabilities, producing a balanced picture of safety significant issues across a broad spectrum.

3.2 What are the Various Levels of PSA ?

The development of PSA over the years has led to three internationally accepted levels of analysis (i.e. Level 1 PSA, Level 2 PSA and Level 3 PSA).

Level 1 PSA

This is the initial and foundation level of a PSA. This level provides an assessment of plant design and operation focusing on those accident sequences which could lead to core damage. It is this part of the PSA which can provide major insights into design strengths and weaknesses, as well as ways into preventing core damage, which in most cases would be a precursor to accidents leading to major radioactive releases with potential health and environmental consequences.

Level 2 PSA

A Level 2 PSA quantifies the magnitude and frequency of radioactive release to the environment following core damage and containment failure. This level of analysis builds on the analyses already undertaken in the Level 1 PSA study.

A Level 2 PSA evaluates accident phenomena, determines different containment failure modes that can lead to radioactive releases (source term), estimates large early release frequency (LERF) and provides insights into the weaknesses and strengths of on site accident mitigation and management measures.

Level 3 PSA

Level 3 PSA evaluates frequency and magnitude of radiological consequences to the public, environment and the society considering meteorological conditions, topography, demographic data, radiological release and dispersion models.

A Level 3 PSA analyses atmospheric dispersion and deposition of radioactive releases, identifies various exposure pathways, estimates health effects on plant workers and the public and also estimates other societal risks and provides insights into the strengths and weaknesses of various possible countermeasures or protective actions. It also provides insights into the adverse effects on the contamination of the land, air, water, and foodstuffs.

Fig. 1 depicts the over view of PSA i.e. Level 1 PSA estimates the frequency of 'core damage', Level 2 PSA estimates the frequency of release categories (source term) and Level 3 PSA estimates the risk to humans (health effects). The 'Risk' is measured in terms of impact/consequence and likelihood of an event. For risk assessment all three levels of PSA are required.

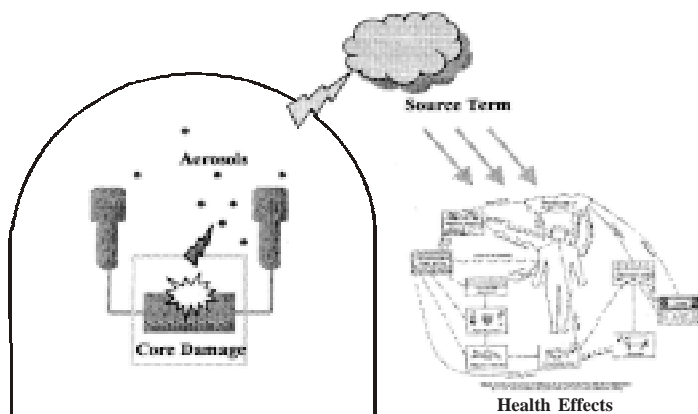


FIG. 1: CORE DAMAGE, SOURCE TERM AND HEALTH EFFECTS

3.3 PSA or PRA ?

The terminology for probabilistic assessment depends on the undesirable outcome being analysed. If the undesirable outcome is early fatalities or injuries, or the number of latent cancer fatalities then the proper terminology would be probabilistic risk analysis (PRA). On the other hand, if the undesirable outcome is core damage, where the public or the environment is still not at risk of being affected, then the terminology would be probabilistic safety analysis (PSA). PRA is primarily used in USA; in other countries most people use PSA. However, now-a-days PSA and PRA are interchangeably used.

3.4 Deterministic Analysis and PSA- ‘Conservative’ or ‘Realistic’ ?

The main characteristics of the deterministic analysis can be described by three major steps namely: (i) identification and categorization of events considered in the design basis, (ii) analysis of the enveloping scenarios and (iii) evaluation of consequences against the acceptance criteria. The PSA also considers the initiating events, which are further analysed along with consequent success and failure combinations of the safety systems using event trees. The end states of the event sequences are assigned different damage categories based on the deterministic analysis results.

In deterministic analysis, enveloping scenarios are evaluated. In PSA also, initiating events are grouped based on the challenges they impose on the safety systems and event tree is developed for the representative event of the group. In fact, design basis event can be viewed as one of the accident sequence of the full event tree model. The common understanding is that deterministic analysis is ‘conservative’ while the PSA is more ‘realistic’. It appears that this is an unnecessary controversy.

The objective of the deterministic analysis is to find out the consequence of the event while that of the PSA is to find out the frequency of occurrence of the particular event and its consequence obtained from deterministic analyses. While concerning the frequency calculations, the PSA is more detailed and ‘realistic’ as compared to deterministic analyses where the frequency estimation is based on the implicit consideration of probability. With respect to the damage estimation the situation is opposite.

The deterministic analyses are performed with two different ways: (i) with conservative methods and assumptions and (ii) with ‘best estimate’ methods and assumptions along with uncertainties. The analyses results of both are more ‘realistic’ than PSA. Both PSA and deterministic methods apply their main power in the aspects they focus: ‘damage’ in deterministic analysis and ‘frequency’ in PSA. In its respective field, each method is more detailed and likely to be more realistic, but in the other’s field both of them use rough approximations.

3.5 PSA and Deterministic Analysis: To What Extent are they Complementary ?

The ultimate goal of the safety analysis is to evaluate the adequacy of the plant protection and defense-in-depth so that the safety functions are fully addressed. The safety analysis can be performed in deterministic or probabilistic ways. There are certain aspects, which are common to both these approaches like selection of postulated initiating events (PIEs). There are certain aspects, in which both methods are complementary to each other that can be summarized as follows:

Element of Approach	Deterministic Approach	Probabilistic Approach
Initiating Events	Limited to DBAs BDBAs are not considered	All potentially important events are considered
Operator Behavior	- No operator action is postulated in first 15/30 minutes following an accident. - No operator errors are postulated after 15/30 minutes.	Human errors in diagnosis and task execution are considered throughout the accident sequence
Failure Analysis	Single failure criterion is applied	Multiple failures and common cause failures are postulated

3.6 Can We Trust PSA ?

Since the PSA model attempts to simulate reality, it is inevitable that there will be simplifying assumptions and idealisations of rather complex processes, phenomena and variability in the data. These simplifications and idealisations will generate uncertainties. These uncertainties limit the usefulness of PSA. However, there are ongoing efforts to improve the accuracy in data used for PSA to minimize uncertainties and to standardize the procedure for performing PSAs. Each source of limitation/uncertainty can be meticulously quantified and therefore these uncertainties can be turned into strength of PSA by performing sensitivity analyses for dominating contributors and PSA results can then be used with high confidence.

While using PSA in regulatory decision-making, both the regulator as well as the operating organization should have adequate competence and experience. The main requirement of the PSA in the 'risk-informed approach' is that the 'quality' of the PSA should be consistent and commensurate with the intended application. The 'high quality' PSA can be prepared if adequate 'quality

assurance plan for PSA' has been established. Other important aspect in regulatory decision-making is that the decision must be based on the full understanding of the uncertainties involved in PSA. This understanding is dependent on the sources of information used in the development of PSA and the adequacy with which the information is documented.

3.7 What Should be the Scope of the PSA ?

Most PSAs for an NPP consider initially modeling of the plant at normal operating conditions at 100% full power with events, which occur internally to the plant and could potentially lead to core damage. The scope could be increased to include internal hazards such as internal fire and internal flood, and external events such as earthquake, external fire, external flood, extreme wind and aircraft crash, etc. and other plant states such as low power operation and shutdown. Further, the scope can be increased to Level 2 PSA to determine the release of radioactivity, which would occur if containment integrity were lost following the core damage. And finally effort should be made to extend the scope to Level 3 PSA to address the health effects to the plant personnel, the members of public and the environmental consequences. However, it is to be recognised that the sources of uncertainties increase with the level of PSA being performed (i.e. uncertainties are more in level 3 PSA as compared to Level 2 PSA and more in Level 2 PSA as compared to Level 1 PSA).

4. ELEMENTS OF LEVEL 1 PSA

4.1 Plant Familiarization and Information Gathering

This is the most difficult and time-consuming activity with respect to producing a PSA. The volume of the information required to be put together in a PSA is enormous and dependent upon numerous aspects. For example whether the PSA is being performed by analysts who already have detailed plant design and operational experience or PSA is performed at design stage or following numerous years of operation. Even if all the information required for a PSA is available it may not be in a form in which it can be used straight away.

One thing is to be borne in mind that the PSA is an interdisciplinary subject. Hence, the team performing PSA should consist of PSA specialist, plant personnel, data analysts and human factor specialists.

4.2 The Selection and Grouping of Initiating Events

This is one of the tasks, which ensures completeness of the PSA within its defined scope, as the omission of one or more events of significance can have a profound effect on the overall results. Within the scope of the PSA, initiating

events are derived from various sources, such as engineering evaluation, reference of previous lists, deductive analysis and operational experiences.

Once the task of assessing the requirements of the plant systems has been completed, the initiating events can be grouped in such a way that all events in the same group impose essentially the same success criteria on the front line system as well as the same special conditions (challenges to the operator, to automatic plant responses, etc.). The main objective of grouping is to arrive at initiating events of manageable number that should represent each group appropriately including bounding cases for PSA modeling.

4.3 Accident Sequence Modeling

This step is the determination of the possible plant responses to each of the defined initiating event groups. This modeling results in the generation of accident sequences with a given consequence, and is normally undertaken using different techniques such as event tree analysis (ETA), cause consequence diagrams etc. A typical event sequence can be expressed in terms of the initiating event and the success or failure of mitigating systems and human responses.

4.4 System Modeling

This provides the detailed modeling of the constituent events of the accident sequences derived from the accident sequence modeling. Fault tree analysis (FTA) is the most widely used method for developing system models. However, other techniques such as markov analysis, reliability block diagrams and go charts can also be used. FTA is a deductive failure analysis, which can be simply described as an analytical technique whereby an undesired state of the system is specified, and the system is then analysed in the context of its environment and operation to find all credible ways in which the undesired state could be brought out.

4.5 Data Acquisition and Assessment

This is the final task prior to quantification of the PSA model. The data (i.e. numbers of occurrences of the events and the total periods over which these events have been observed) are required as input in determining initiating event frequencies for input into the event trees. The data (i.e. component failures, repair, test, maintenance and common cause failure data and human error data) are required for input into the fault trees. For each of these, the identification of data sources and data collection is required, together with the selection and application of estimation techniques. Sources of such data are the plant logbooks, in which 'significant occurrences' are recorded, and licensee event records. If adequate plant-specific data are not available, then the 'generic' data can also be used with Bayesian Update technique.

Multiple failure of events (caused by internal equipment failures and multiple failures due to clearly identifiable human errors) for which a clear cause-effect relationship can be identified should be explicitly modeled in the fault tree model. Multiple failures, for which no clear root cause event can be identified, can be modeled using common cause failure (CCF) models such as b-factor, a-factor, multiple greek letter (MGL) or binomial failure rate (BFR) model.

Human caused failures also should be included in the fault tree/event tree models and human error probabilities should be estimated using various human reliability analysis models such as time independent model-technique for human error rate prediction (THERP), time dependent model- human cognitive reliability (HCR), and operator action tree (OAT) etc.

4.6 Accident Sequence Quantification

This is the culmination of all the previous tasks of the PSA. Quantification using the Boolean algebraic solutions associated with the event tree/fault tree analysis is undertaken for determining the relative importance to the core damage frequency (CDF) of the various contributors. Where conservative estimates of input data or modeling assumptions appear as dominant contributors, further refinements to these data and assumptions may be required and the appropriate sequences are requantified in order to achieve an overall balanced PSA model.

5. ELEMENTS OF LEVEL 2 PSA

For Level 2 PSA few more specific steps needs to be performed than Level 1 PSA. The major steps involved in Level 2 PSA are described below.

5.1 Identification of Plant Damage States

Level 1 PSA identifies a very large number of accident sequences, which may lead to core damage. The end states of these sequences are obtained from deterministic analyses and assigned with different core damage categories. These sequences are very large in number. For Level 2 PSA the accidents are further analysed and for each of these accident, containment performance evaluation and source term needs to be estimated. Hence, these sequences are grouped together into plant damage states (PDSs) so as to reduce the number of scenarios to the manageable number. PDSs group these sequences such that each PDS would have similar effects on containment response and fission product source terms. The grouping is done based on the initiator type (e.g., large LOCA transients), reactor coolant system pressure at core damage, status of emergency core cooling system, status of containment's

engineered safety features, and status of primary and secondary containment (like isolation/ bypass failure).

5.2 Accident Progression and Containment Analysis

The purpose of the accident progression and containment analysis is to track the physical progression of the accident further from the PDSs until it is concluded that no additional release of radioactive material from the containment building will occur. The analysis tracks the impact of the accident progression on the containment building structure, with particular focus on the threat to containment integrity posed by pressure and temperature loadings or other physical and chemical phenomena.

For example, for boiling water reactors (BWRs), the phenomena can be divided into three stages: (i) phenomena within reactor pressure vessel (RPV) and reactor coolant system (RCS), (ii) phenomena within reactor cavity/vault and (iii) phenomena within containment building. For pressurized heavy water reactors (PHWRs) these can be divided into four stages: (i) phenomena within reactor coolant circuit, (ii) phenomena within calandria, (iii) phenomena within the calandria vault and (iv) phenomena within containment building.

Some of the accident phenomena are: core-concrete interaction (CCI), high pressure melt ejection (HPME), direct containment heating (DCH), steam explosion, hydrogen generation, deflagration and detonation etc. These are highly complex set of physical and chemical phenomena. In Level 2 PSA these phenomena are not described fully as for many of these phenomena, complete understanding is still going on as research activities. However, the phenomena are placed within overall structure of Level 2 PSA to account for their potential effects on the containment integrity. These approximations contribute to uncertainty in Level 2 PSA results.

5.3 Development of Accident Progression Event Trees

The plant-specific analyses of the progression of severe accidents are performed using Level 2 PSA computer codes or in-house developed computer codes. In addition, if available, literature for similar plants and containments could be used as a basis for establishing an adequate framework for the accident progression event trees (APETs)/containment event trees (CETs). These are similar to event tree models used in Level 1 PSA in principle. Once the APETs are developed, the next step is to assign proper nodal probabilities to each branch point in APETs. The determination of conditional probabilities (at each branch point) is based on deterministic analyses and expert judgement. The quality of this expert judgement is dependent on the analyst's current state of knowledge to a particular issue.

5.4 Source Term Analysis

A source term (ST) is defined as the quantity, timing, duration and

characteristics of the release of radioactive material to the environment following a postulated severe reactor accident. The core of a power reactor contains several million curies of radioactivity of hazardous nuclides built up during equilibrium power operation. Several barriers (e.g. fuel matrix, fuel cladding, reactor coolant system and reactor containment) must be breached before any significant part of this radioactivity can be released to the environment. Establishing the timing and nature of the breaching of these barriers is an essential part of ST analysis.

The aim of the ST analysis is to find out what part of the activity originally released from the core will be retained in different areas of the plant, and what will escape. Early containment failures are usually associated with high source terms. On the other hand, a delayed containment failure will ensure that a good part of the radioactivity reaching the containment is retained therein. It must be pointed out that the possibility of containment bypass must be established, for that would result in high ST scenarios even when the reactor has a strong containment and its integrity is not lost.

5.5 Estimation of Frequencies for Release Categories

Once the APETs are developed, reliability of containment-engineered features is to be evaluated and integrated with APETs along with the other nodal probabilities. The analyst with the help of computer codes, evaluate the frequency of the accident sequences originated from all the PDSs. As in Level-1 PSA, here also large number of end states would result, some of which are identical in terms of key release attributes. Depending upon the similar characteristics, these end states are grouped together in terms of different release categories. For each of these release categories, the corresponding frequency can be calculated and from these the risk measure of Level 2 PSA and large early release frequency (LERF) can be evaluated.

6. ELEMENTS OF LEVEL 3 PSA

Level 3 PSA takes input from the Level 2 PSA results and estimate the risk to the public by performing few more specific steps. The major steps involved in Level 3 PSA are described below.

6.1 Interface with Level 2 PSA

The starting point of Level 3 PSA is the 'Source Term' information provided by a Level 2 PSA. This information is provided for each of the representative accidents to be assessed, obtained by grouping accidents with similar release characteristics together. The important attributes of the source term such as

timing and duration of releases, height of release and thermal energy associated with releases are the direct input for the second step of the Level 3 PSA.

Other characteristics of release (the physical form and chemical properties of radionuclides) are assumed to be constant in all release cases. It is assumed that they are released in oxide form as aerosol particle with 1 μ m activity median aerodynamic diameter (AMAD) or one can use available distribution of aerosol size, except noble gases, which appear in elemental form, and iodine, which may appear in elemental, organically bound and particulate forms.

6.2 Atmospheric Dispersion and Deposition

Material released to the atmosphere is transported downwind and dispersed according to normal atmospheric mixing processes. The diffusion-transport equation is commonly used for estimating dispersion in the atmosphere. For this, meteorological data is required to be obtained. It is a normal practice to use the meteorological data from the meteorological station nearest to the release point. Data compiled at other stations may, however, be acceptable if they are representative of the general condition experienced by the plume.

The atmospheric dispersion and dose calculation are repeated for a large number of sequences of conditions selected from the meteorological data file used to predict the full distribution of consequences, which may occur. Ideally the calculation may be performed for every possible sequence of weather conditions in the data file, in other words a weather sequence at each hour on the file. It is neither practicable nor necessary to consider every such sequence. Instead, the one or more year's data is sampled in such a way that a truly representative set of weather sequences is selected. The selection should be made in such a way that the sequences chosen represent the complete set of possible sequences, and yield the correct probability distribution of consequences.

Once these data are obtained, atmospheric dispersion and deposition of the radionuclides are modeled. Several models have been developed for this purpose using a variety of boundary conditions and simplifying assumptions. Many simple theoretical formulations of dispersion predict that concentration profile will have a Gaussian shape. Additionally, they assume that the downwind transport goes along a straight line. Although the assumption of simple theories does not hold for real atmosphere, the Gaussian shapes have been found empirically to be approximately valid in many situations and it forms the basis of the Gaussian plume model which has been, and still is, widely used in consequence assessment.

6.3 Identification of Different Exposure Pathways

There are six principal pathways (i.e. external β and γ irradiation from the radioactive materials in the cloud, inhalation of radioactive materials in cloud,

external dose from radioactive material deposited on skin and clothing, external irradiation from deposited radionuclides on ground, inhalation of resuspended material and ingestion dose) by which people can accumulate a radiation dose after an accidental release of radioactive materials to the atmosphere. For each pathway a dosimetric model is required to convert the concentration of radionuclides in the atmosphere, on the ground, in foodstuffs, or on skin and clothing to dose to humans.

6.4 Dose Evaluation

Once the exposure pathways are identified, the doses received by the humans are required to be calculated from each of these exposure pathways to find out the risk. Different dose conversion factors such as attenuation factor, shielding factor, re-suspension factor etc. are used for this purpose.

6.5 Countermeasures

A variety of possible countermeasures or protective actions may be taken following an accidental release to reduce the impact of the accident on the environment and the public. For realistic estimate of the exposure of the population, appropriate account of these countermeasures is taken in the risk evaluation task of Level 3 PSA.

The various protective actions available fall broadly into two categories depending upon the time at which they are implemented and the effects for which they are designed to mitigate: short-term protective actions and long-term countermeasures.

Short-term countermeasures include sheltering, evacuation, the issuing of stable iodine tablets, and the decontamination of people. The primary objective of such measures is to limit the exposure of the population to both internal and external irradiation with the intention of preventing deterministic effects and minimizing risks of stochastic effects.

Long-term countermeasures include changes to agricultural practices, deep ploughing, alternate feed, cesium binders, alternative crops and alternate production. Long-term countermeasures are designed to reduce chronic exposure to radiation, both externally from deposited material and internally from ingestion of contaminated food, with the intention of reducing the incidence of late health effects.

6.6 Estimation of Health Effects and Other Risks

The exposure of individuals to ionizing radiation can lead to health effects, which are generally classified as either 'deterministic' or 'stochastic'. Deterministic effects and stochastic effects are often referred to as 'early' effects and 'late' effects, respectively. Effects observed in exposed individuals,

i.e., deterministic effects and cancers are termed 'somatic' effects, while those observed in their descendants are known as 'hereditary' (genetic) effects. Different models are available for this purpose.

The most common risk measure of Level 3 PSA is presented in the form of complementary cumulative distribution functions. An example is shown in Fig.2.

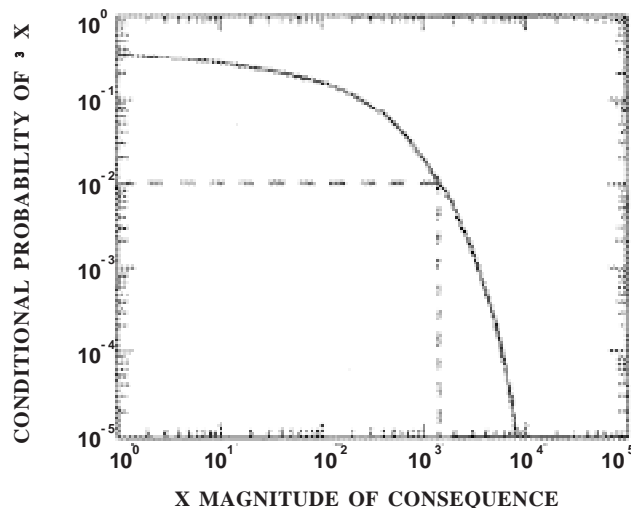


FIG. 2: AN EXAMPLE OF CUMULATIVE DISTRIBUTION FUNCTION

The ordinate of these cumulative distribution function (CCDF) is the probability of equaling or exceeding the consequence magnitude indicated by the curve. The abscissa is the numerical value of the consequence, which may be any of the effects, such as number of early fatalities or injuries, the number of latent cancer fatalities, the size of the area contaminated to such a level that decontamination is required, and so on. Logarithmic scales are employed on both axes to accommodate the wide range of frequencies and consequences involved. CCDFs are often used as a measure of public risk. In addition, the expected (mean) value of the CCDF (which corresponds to the integral of the CCDF) is frequently used as a summary measure of risk.

7. COMPUTER CODES USED FOR PSA

A number of computer codes and software packages are currently used for performing PSA. Typically, an integrated software package is used in the Level 1 PSA analyses for the development and storage of system models, sequence models, failure data, and sequence quantification. Level 2 PSA and Level 3 PSA analyses will also require the use of large computer codes. Finally, smaller pieces of software may be used for special analyses, conversion or transport of data. Increasingly, integrated software packages are developed and used, covering almost all levels and tasks of a PSA.

In order to ensure quality assurance (QA) for the PSA, all computer codes used in the development of the PSA must be verified and validated, either in the course of their development or by the PSA group. Computer codes that are available commercially may be verified and validated by the code developer. For software that is not commercially procured but, for example, written internally in the PSA organization, a verification, validation and QA process should be performed.

7.1 Computer Codes used for Level 1 PSA

Some of the computer codes, which are used for Level 1 PSA studies are:

Risk Spectrum PSA Professional

IRRAS

SAPHIRE

PSA PACK

ISOGRAPH

7.2 Computer codes used for Level 2 PSA

Some of the deterministic computer codes, which are used for assessing the accident consequence for input in Level 2 PSA studies are:

MELCOR

MAAP

THALES

ATHLET-CD

STCP

7.3 Computer Codes Used for Level 3 PSA

Some of the computer codes which are used for Level 3 PSA studies are:

ARANO

CONDOR

COSYMA

MACCS

8. APPLICATIONS OF PSA

PSA can be used to explore the risk significance of various aspects of NPP design and operation, the risk impact of changes in NPP design or modification of operating procedures and for the evaluation of the abnormal events that occur at NPP. To use PSA for such applications, PSA should be performed with state-of-the-art methodology and should be updated with respect to the changes/modifications in plant configuration and reliability data obtained from the plant experience. The following are the PSA applications:

8.1 PSA Applications for Design of NPPs

This is the most important application of PSA as it helps to identify design deficiencies that can challenge plant safety during the operation phase. PSA can be used at design stage of NPPs. However, it is to be understood that the PSA for a new plant design would contain substantial uncertainties due to incomplete information of design details, limited database, reliance on preliminary procedures, preliminary thermal-hydraulic analyses, etc. Hence, the PSA analysis at design stage should be supported with uncertainty and sensitivity studies. Some PSA applications during NPP design are:

8.1.1 To Support NPP Design

A PSA provides a fully integrated model of the entire plant that can be used to examine the risk from a variety of possible initiating events (e.g. transients, LOCA, support system failures, etc.). The model combines front-line safety systems and support systems in a manner that allows designers to identify the risk significance of important inter-system dependencies. The PSA allows designers to examine the significance of single failures and multiple failures, and to determine the risk importance of 'safety', 'safety related' and 'non-safety' systems. Consideration of only a limited set of design basis accidents and application of traditional deterministic design criteria for individual safety functions, systems, and components do not provide the same benefits as the combination of traditional approaches and PSA.

8.1.2 To Support NPP Upgrade and Backfitting Activities and Plant Modifications

One of the major goals of PSA is to assess the level of safety of existing plants and to identify design weaknesses that need to be corrected by plant improvements (backfits). If the frequency of core damage or severe off-site releases is largely dominated by a very limited number of accident sequences, effective backfits may be proposed to prevent or to mitigate these scenarios. Proposed backfits may involve changes to system designs and installation of new hardware. They may also involve changes to operational procedures, development of specific accident management procedures, etc. PSA

evaluations can also be used to demonstrate which modifications are acceptable and to compare or suggest possible alternatives.

8.2 PSA Applications for Operation of NPPs

PSA can provide valuable insights for the NPP operation. It provides the framework for risk-informed operational activities. Some of the applications of PSA in NPP operation are as follows:

8.2.1 Tool as a Safety/Risk Monitor

A safety/risk monitor is 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 safety monitor reflects the current plant configuration in terms of the known status of the various systems and/or components, e.g. whether there are any components out of service for maintenance or tests. It is necessary to control the risk due to plant configurations during power operation as well as during the shutdown state of the plant.

There are two main tasks in the risk based configuration control, risk planning and risk follow-up. Risk planning is a forward-looking application of PSA and it consists of supporting the preparation, planning and scheduling of plant activities and configurations. This application can be performed with an on-line or off-line PSA model. Risk follow-up involves the online use of the PSA by plant personnel in order to keep the risk due to actual configurations, plant activities and unanticipated events, at an acceptable level.

8.2.2 Evaluation of Technical Specifications for Operation

Technical specifications for operation (TS) are operating rules for NPPs that are approved by the regulatory authority. The technical specifications define limits and conditions for operations, testing, and maintenance activities as a way to assure that the plant is operated safely in a manner that is consistent with the plant safety analyses. The TS define limiting conditions for operation (LCOs) and surveillance requirements (SRs).

LCOs also define equipment operability requirements and allowed outage times (AOTs). Surveillance requirements define the safety system and safety related/supporting systems testing requirements and the surveillance test intervals (STIs). PSAs can be used to develop quantitative bases for optimized limits on equipment AOTs, STIs and testing strategies.

8.2.3 Periodic Safety Review

A safety assessment process consists of identifying safety issues, determining their safety significance and making decisions on the need for corrective measures. This has to be done continuously during the life of the plant. In

practice however, a major safety review is normally performed periodically, e.g. every 10 years.

A major benefit of including PSA in periodic reviews is the creation of an up-to-date overview of the whole plant. If an older plant cannot be shown to totally comply with current safety standards, PSA results can sometimes be used to help justify continued operation. The PSA review may well lead to the identification of real cost-effective improvements to safety. Frequently, the incorporation of data resulting from operating experience into the PSA to replace conservative design assumptions will lead to a relaxation of operating constraints, while still maintaining adequate safety margins.

8.2.4 Severe Accident Management and Emergency Planning

While the emergency operating procedures direct operation of the plant in controlling the progression of an accident, the realm of severe accident management is entered where any other possible means, internal or external, of mitigating the accident and its consequences may be utilized. PSA is a good source available to identify accident sequences, to categorize them into functional groups, and to provide descriptions of plant responses and vulnerabilities. PSA can support the development of strategies to deal with the identified vulnerabilities and of calculational aids that would be used to assist in the selection and application of the strategies.

8.2.5 Risk-informed Inspections

The main objective of the regulatory inspection is to ensure continued operation of NPPs while maintaining the adequate safety. These inspections are carried out with different objectives. For example, an inspection can be carried out for resolution of generic safety issues assuring adequate safety improvements. The special inspection can be carried out when declining performance of NPP is noted. An inspection can be carried out in response to operational events when deemed necessary.

The PSA can be a useful tool in 'risk-informed' regulatory inspections. The objective of the risk-informed inspection is not to replace the traditional inspection process but to enhance/balance the existing inspection process. The risk-informed approach improves the effectiveness and efficiency of the inspections by focusing the resources on the risk-significant aspects. The PSA insights are useful in identifying the important risk contributors (i.e. components as well as important human actions). This information is used to identify the inspectable areas in base-line inspections. The PSA can also be used to find out the risk impact of the inspection findings/operational events. This is known as 'significant determination process'. Depending upon the level of significance, other inspections such as special inspection, generic safety inspection and event response can be supplemented.

9. ROLE OF PSA IN THE REGULATORY DECISION MAKING

Traditionally, NPPs have been designed, constructed and operated mainly based on deterministic safety analysis philosophy. In this approach, a specific set of postulated initiating events are analysed and their consequences are evaluated to establish design and operational requirements. To account for the uncertainty, a substantial amount of safety margin is incorporated. In spite of all these considerations, experience has shown that there are certain accidents, which fall outside the domain of traditional design basis accident (i.e. multiple failures at TMI-2 and fire incident (external event) at Browns Ferry). Hence, to cover such scenarios a more integrated approach is required.

The PSA provides a methodical approach in identifying accident sequences that can result from a broad range of initiating events. It includes the systematic determination of accident frequencies and consequences, and aims as much as possible to be 'best-estimate'. However, since the PSA model attempts to simulate reality, it is inevitable that there will be simplifying assumptions and idealisations of rather complex processes, phenomena and variability in the data. These simplifications and idealisations will generate uncertainties, which limit the usefulness of PSA.

For best utilization of the advantages of both these approaches, an integrated approach should be used for decision making. In view of this, many regulatory bodies desire to move towards an approach in which PSA insights are used as one of the inputs along with other inputs such as the degree to which any mandatory requirements are met, the insights from the deterministic analysis, the results of the cost-benefit analysis etc. This is known as 'risk informed decision making' (RIDM).

If the results of the PSA are to be used in RIDM, it will be necessary to formulate some form of acceptance criteria (i.e. quantitative goals). The quantitative goals should be developed under the leadership of the regulatory body through a process of consultation between the regulatory body and the licensees/utilities. Maximum use should be made of experience available within the industry, knowledgeable experts, national and international expert bodies.

In order to be useful as a regulatory tool, PSA models will have to meet certain requirements. The scope of the PSA, in terms of the coverage of the contributors to risk must be sufficient for the proposed applications. To the extent possible, plant specific PSAs based on state of the art, 'best-estimate' models, assumptions and data should be used. PSA model should be developed to a level of detail such that dependencies and failure modes applicable to the decision are adequately modelled.

10. ISSUES FOR ADVANCEMENT OF PSA

PSA methodology has been under continuous improvement since its origin. The state-of-the-art has now matured for at least Level 1 PSA with internal events. Still there are certain areas in which world wide consensus have not been arrived at. There are large variabilities in the fault tree and event tree modeling. Not much work has been reported regarding the validation aspects of PSA methodology. Some PSA standards have been developed and basic elements of PSA are standardized. However, some modeling issues are not fully addressed yet. The important issues are as mentioned below:

- Validation of PSA
- Development of probabilistic safety criteria
- Assessment and incorporation of safety culture in PSA
- Use of human reliability analysis in PSA
- CCFs across the safety systems
- Modeling of shared systems
- Modeling of computer based systems
- Integration of passive systems in PSA
- Incorporation of ageing effects in PSA

APPENDIX-A

GENERAL METHODOLOGY FOR LEVEL 1PSA

A1.1 Fault Tree Analysis

A fault tree (FT) analysis can be described as an analytical technique, whereby an undesired state of the system is specified, and the system is then analysed in the context of its environment and operation to find all credible ways in which the undesired event may occur. The FT is a graphical model of the various parallel and sequential combinations of fault that will result in the occurrence of the predefined undesired event. The fault can be component hardware failures, human errors, or any other pertinent events, which can lead to the undesired event. A fault tree thus depicts the logical interrelationships of basic events that lead to the undesired event.

It is important to understand that a FT is not a model of all possible system failures or all possible causes for system failure. It is tailored to its top event, which corresponds to some particular system failure mode, and the FT thus

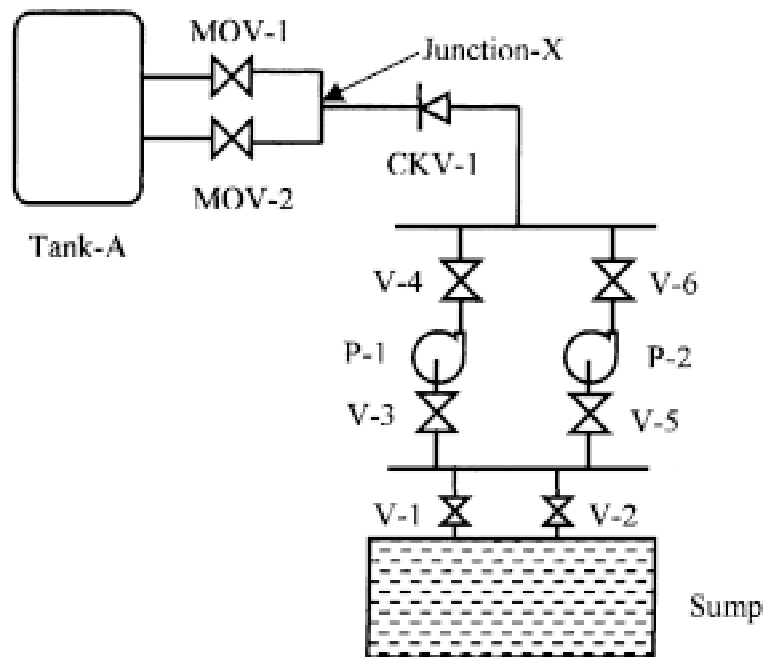


FIG. A1 : WATER SUPPLY SYSTEM

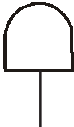


includes only those faults that contribute to this top event. Moreover, these faults are not exhaustive. They cover only the most credible faults as assessed by the analysts.



In constructing a fault tree, the basic concepts of failure effects, failure modes and failure mechanisms are important in determining the proper interrelationships among the events. The failure mechanisms produce failure modes, which, in turn, have certain effects on system operation. To illustrate these concepts consider a simple system that supply the water from a sump to a tank-A. The system consists of a sump, two pumps, one check valve, two motorized valves, tank-A and associated piping. This is shown in Fig. A1.

A1.2 Fault Tree Gates and Symbols

Before the fault tree is constructed, let us first understand the basic fault tree gates and symbols used in the fault tree models.

TABLE-1 : BASIC FAULT TREE GATES AND SYMBOLS

	AND Gate	<p>The AND gate is used to indicate that the output occurs if and only if all the input events occur. The input events can be basic events, intermediate events (outputs of other gates), or a combination of both. There should be at least two input events to an AND gate.</p> <p>Summary of logic : All events must be TRUE for the output to be TRUE.</p>
	OR Gate	<p>The OR gate is used to indicate that the output occurs if and only if at least one of the input events occur. The input events can be basic events, intermediate events, or a combination of both. There should be at least two inputs to an OR gate.</p> <p>Summary of logic : If at least 1 event is TRUE, the output is TRUE.</p>
	Transfer Gate	<p>A transfer gate is a symbol used to link logic in separate areas of a fault tree. There are two primary uses of transfer gates. First, an entire fault tree may not fit on a single sheet of paper or you may want to keep the individual trees small to view and organize them. Second, the same fault tree logic may be used in different places in a fault tree.</p>

	Basic Event	A basic event is either a component level event that is not further resolved or an external event. It is at the lowest level in a tree branch and terminates a fault tree path.
	Undeveloped Event	An undeveloped event is used if further resolution of that event does not improve the understanding of the problem, or if further resolution is not necessary for proper evaluation of the fault tree. It is similar to a basic event, but is shown as a different symbol to signify that it could be developed further but not done so for the analysis.

A1.3 Procedure for Construction of Fault Tree

Before constructing a fault tree of any system, a very good understanding of the system operation as well as the operation of its components and the effects of their failure on system success is necessary. Clear and precise definitions of system boundaries need to be established before the analysis begins. Once this is done, the fault tree can be constructed. A typical fault tree for the system illustrated in Fig. A1 is developed in Fig. A2.

First the analyst needs to define the top event. In this case, let the top event is defined as: 'system fails to supply water to Tank-A'.

The next step is to determine the immediate, necessary, and sufficient causes for the occurrence of the top event. These may not be the basic causes of the event but the immediate causes or immediate mechanisms for the event. These immediate causes are treated as sub-top events and the analyst needs to proceed to determine their immediate, necessary and sufficient causes to limit of resolution of the fault tree. This limit consists of basic component failures of one sort or another. This approach of constructing a fault tree is known as 'immediate cause' concept.

A1.4 Event Tree Analysis

Event trees (ET) are graphic models that order and reflect event sequences. A typical accident sequence consists of a PIE group, specific system failures and successes, and their timings and human responses. An event sequence can lead either to a successful state or to core damage. Every accident sequence that does not lead to successful end state (safe reactor shutdown state as defined in the plant design and technical specifications for plant operation) is assumed to lead to core damage.

Events or 'headings' of an event tree can be any or combination of safety function, safety systems, basic events and operator actions. The event tree

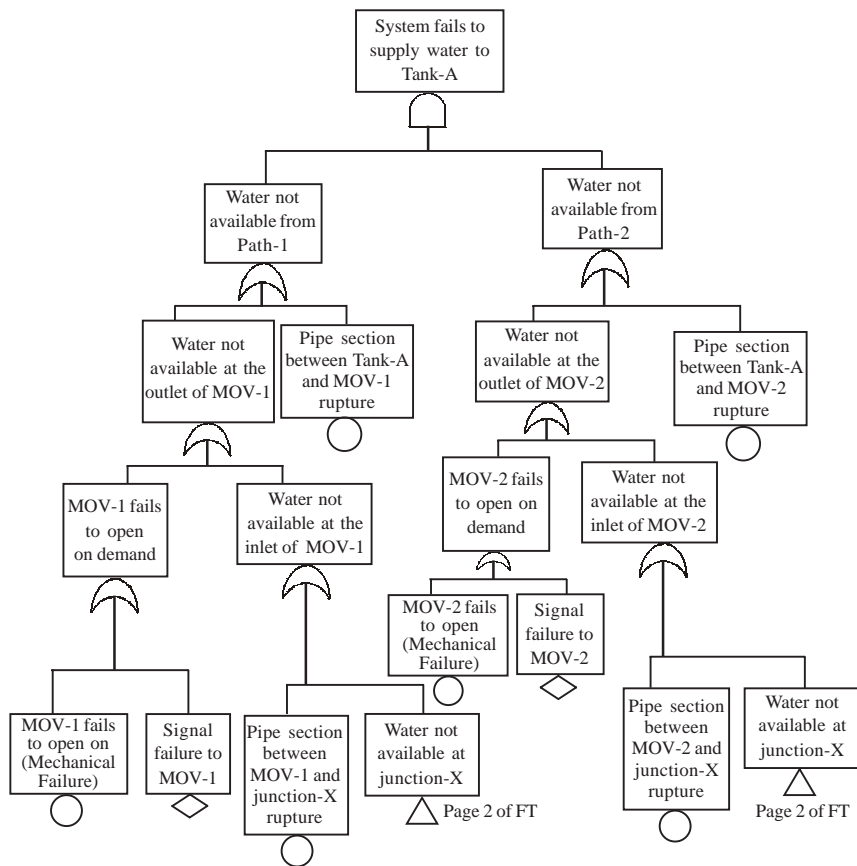


FIG. A2: TYPICAL FAULT TREE FOR WATER SUPPLY SYSTEM (PAGE 1 OF FT)

headings are normally arranged in either chronological or causal order. Chronological ordering means that events are considered in the chronological order in which they are expected to occur in an accident as depicted in (deterministic) safety analysis. Causal ordering means that events are arranged in the tree with 'cause' relationship of the preceding to the successive events.

Before constructing, an event tree the analyst needs to identify various initiating events. The chronological plant responses to each of these initiating events need to be understood. Once this is done, an event tree can be constructed. A typical event tree is presented in Fig. A5 for a typical pressurized heavy water reactor design.

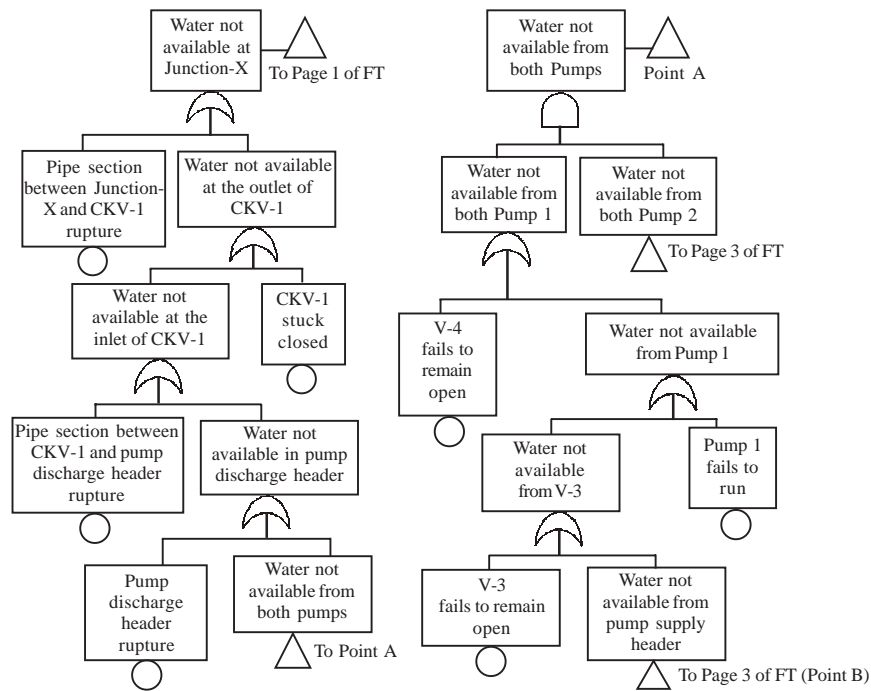


FIG. A3: FAULT TREE FOR WATER SUPPLY SYSTEM (PAGE 2 OF FT)

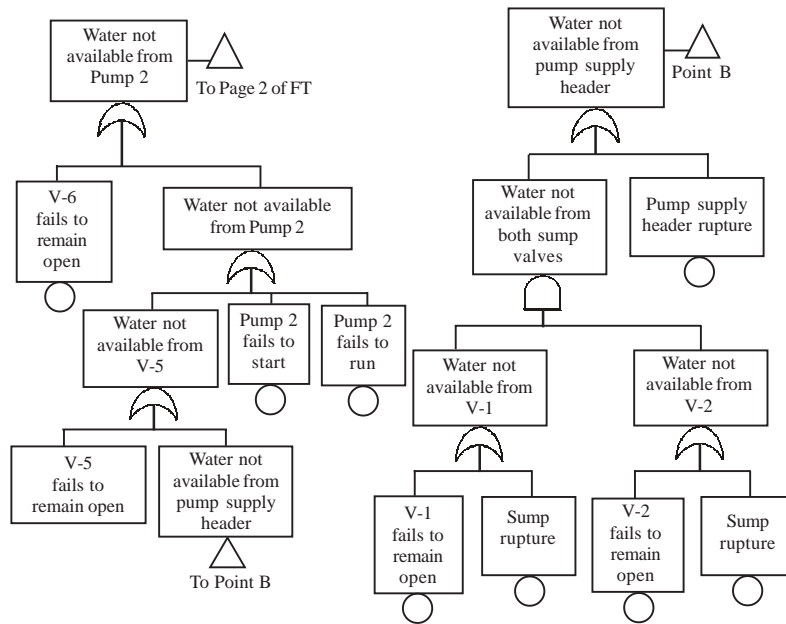


FIG. A4: FAULT TREE FOR WATER SUPPLY SYSTEM (PAGE 3 OF FT)

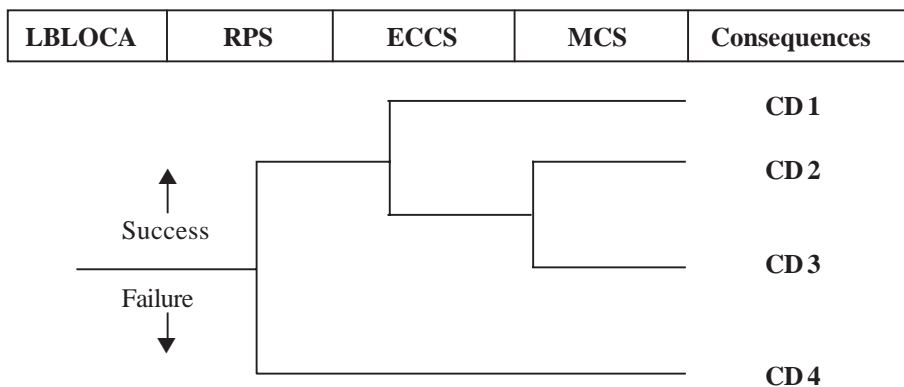


FIG. A5: A TYPICAL EVENT TREE

- LBLOCA: Large break LOCA
- RPS: Reactor protection system
- ECCS: Emergency core cooling system
- MCS: Moderator circulation system
- CD1: Core damage category 1
- CD2: Core damage category 2
- CD3: Core damage category 3
- CD4: Core damage category 4

Here in this illustrative event tree, large break LOCA event is considered as an initiating event. During any accident condition, the first action required for nuclear safety is the reactor shutdown and maintain the reactor under long-term sub-critical state. Hence, in the event tree development, after the initiating event, RPS is used as event tree heading. At each event tree branch point, two paths are developed. The upper path is normally considered as 'success' and the downward path is considered as 'Failure' of the function/system considered in the event tree heading.

If at this stage RPS is considered successful, the second function needs to be ensured for the safety. The second important function during the large break LOCA scenario is to provide long term core cooling. These can be achieved through ECCS or MCS. Hence, the second event tree heading is ECCS. If at this stage ECCS is considered to be successful, there could be some fuel failures and corresponding consequence category is assigned as CD 1. If at this stage ECCS is considered to be a failure, then there is another level of defense for the decay heat removal from the fuel through MCS. If at this stage MCS is considered successful, then limited fuel failure occurs. The corresponding consequence category assigned is CD 2. If at this stage MCS

is considered failure, then large fraction of fuel failure occurs. The corresponding consequence category assigned is CD 3

If after large break LOCA, RPS is considered to be failure then the core structural integrity cannot be maintained due to large amount of positive reactivity addition. The corresponding consequence category is assigned as CD 4.

A1.5 Quantitative Risk Assessment of Level 1 PSA

As mentioned above, event trees are needed to be developed for all previously identified initiating events and appropriate consequence category need to be assigned to each end states of the accident sequences. The fault tree analyses need to be carried out for all the safety, safety-related systems that are included in the event tree models.

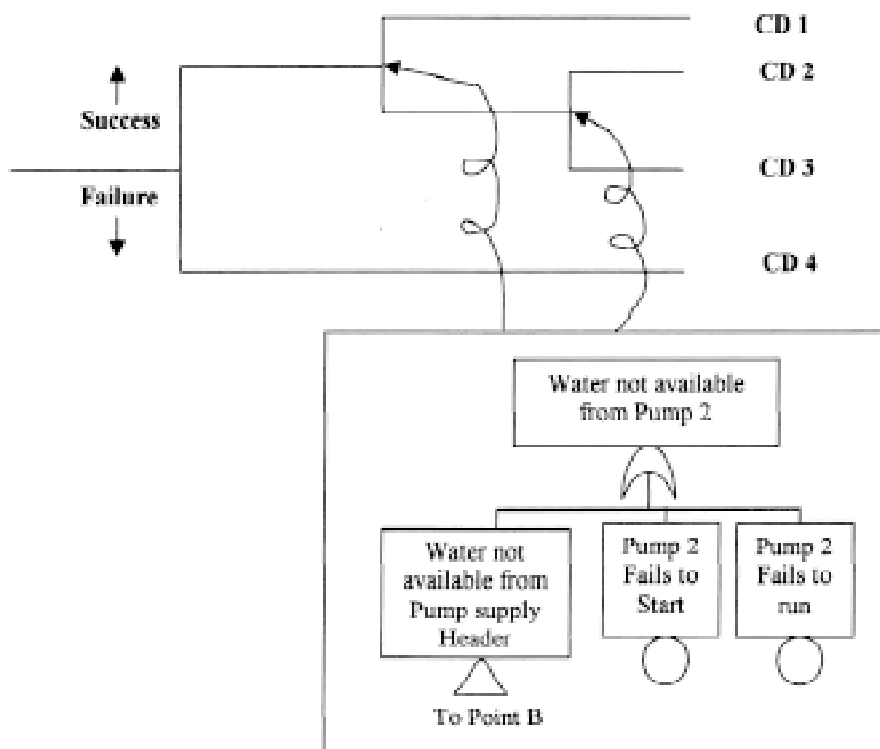


FIG. A6: INTEGRATION OF FAULT TREE MODELS INTO EVENT TREE

Once, this is done, the quantitative risk assessment can be done by integrating the fault tree models into the event tree models appropriately. This is illustrated in Fig. A6. Using the computer code, the analyst evaluates the frequency of all the accident sequences for the different consequence categories. The risk

measure for Level-1 PSA study is the core damage frequency (CDF). This is calculated as follows:

Step 1: Calculation of contribution of individual initiating event (say IE-1) to a particular consequence category (say CD1)

Contribution of IE-1 to CD 1 =

$$\sum_{i=1}^N (\text{Frequency of accident sequence originated from IE-1})_i$$

where, N is the total number of accident sequences originated from IE-1

Step 2: Calculation of contribution of all initiating events to a particular consequence category (say CD 1)(i.e. summed frequency of CD 1)

Summed frequency of CD 1 =

$$\sum_{j=1}^M (\text{Contribution of different IEs to CD 1})_j$$

where, M is the total number of initiating events.

Step 3: Calculation of summed frequency of core damage

Summed frequency of all consequence category (i.e. overall CDF) =

$$\sum_{k=1}^C (\text{Summed frequency of different CDs})_k$$

where, C is the total number of core damage categories.

CONCLUDING REMARKS

PSA is a methodical and logical tool for deriving numerical estimates of risk from a nuclear power plant (or indeed any plant in general). It provides a methodical approach to identify accident sequences that can result from a broad range of initiating events and provides estimates of accident frequencies and consequences. The salient points about the PSA are put forward as:

- Since the PSA model attempts to simulate reality, it is inevitable to avoid uncertainties. However, PSA systematically addresses the uncertainty involved in the quantification of risk. Regulatory decision making using PSA must be based on the full understanding of these uncertainties.
- There is a growing consensus worldwide about the usefulness of PSA in regulatory decision making under the framework of 'risk-informed regulation' approach.
- There are certain areas in PSA for which worldwide consensus have not been arrived at and advancement is needed.

ACKNOWLEDGEMENTS

The authors are grateful to Shri S. K. Sharma, Chairman, AERB for his suggestion for preparation of this monograph and subsequent encouragement and guidance.

They also acknowledge support and valuable suggestions provided by Shri S. K. Chande, Vice- Chairman, AERB during the preparation of this monograph.

Sincere thanks are due to Shri P. Hajra, Chairman, AERB's Committee on PSA, Dr. P. V. Varde, Research Reactor Safety Division, BARC, Dr. S. K. Gupta, Director, SADD, Dr. Om Pal Singh, Director, ITSD, Shri R. I. Gujarati, Director, NPSD, Shri R. Venkatraman, Director, OPSD, Shri R. Bhattacharya, Head, IPSD, Shri K. Srivasista, SADD, Shri J. Koley, OPSD, Shri Utkarsh S. C, NPSD, Shri R. S. Rao, SADD and Shri L. N. Valiveti, IPSD for their review and providing very important comments.

Published by : Atomic Energy Regulatory Board
Niyamak Bhavan, Anushaktinagar
Mumbai - 400 094
INDIA.