Probabilistic Safety Assessment in Nuclear and Non-nuclear Facilities: In a Glimpse

Gopika Vinod

1 Probabilistic Safety Assessment of NPPs

1.1 Introduction to Nuclear Safety

The main goal of nuclear safety is to keep the radiation exposure of the public and workers from nuclear facilities as low as reasonably achievable both during normal operational states and in the event of an accident. NPP safety can be assessed both by deterministically and probabilistically. In the deterministic safety analysis, design basis accidents are considered and it is shown that the engineered safety features provided to counter act such accidents result in radiation doses/risks that are acceptable. In contrast, probabilistic safety assessment (PSA) includes all possible accident scenarios and their quantification in terms of plant damage frequency and consequences. PSA is one of the probabilistic tools available to deal the safety of NPPs probabilistically. This chapter mainly focuses on PSA aspects of NPPs. Probabilistic Safety assessment (PSA) provides a comprehensive and structured approach in identifying failure scenarios that pose potential hazards to the plant, its personnel, environment and the public at large. PSA provides valuable insight into potential weak links in the defence in depth concept. PSA is associated with models which predict offsite radiological releases resulting from potential accidents. It deals mainly with the identification of accident sequence applicable to the design of a reactor and further relegating the risk to various process and safety systems and down to the components and operator actions. In fact it is possible to rank the systems and components in terms of their risk significance. In short PSA is an analytical technique for integrating diverse aspect of design and operation in order to assess the risk of a particular nuclear power plant and to develop an information base for analyzing plant specific and generic issues.

G. Vinod (✉)
Reactor Safety Division, Bhabha Atomic Research Center, Trombay, India
e-mail: vgopika@barc.gov.in

D. R. Karanki et al. (eds.), *Advances in RAMS Engineering*,
Springer Series in Reliability Engineering,
https://doi.org/10.1007/978-3-030-36518-9_15

The risk in general for Nuclear Power Plant (NPP) [1] is defined as:

$$\begin{aligned} Risk &= Likelihood\,of\,occurrence\,of\,undesirable\,event\,(an\,accident) \\ &\times\ Its\,consequences\,in\,terms\,of\,exposure\,to\,radioactive\,material\,release \end{aligned}$$

Therefore the objectives of the nuclear safety are:

- Reduce the likelihood of occurrence an accident
- Minimize the release of radio-active material if accidents happen
- Minimize the population exposure if radio-active materials are released.

The first report on Nuclear Power Plant (NPP) accidents WASH 740 [2] was issued in 1957. The consequences predicted were unacceptable at that time. The importance of this report felt only after Three Mile Island NPP accident, since that accident was predicted in this report. Now PSA study of Nuclear Power Plants are carried out in many countries and are mandatory requirement by their regulatory bodies.

1.2 Probabilistic Safety Assessment for NPP

For carrying out PSA of NPP, three levels of PSA are used [3].

1.2.1 Level 1 PSA

Level 1 PSA deals with the assessment of plant failures leading to the determination of core damage frequency. It provides insights into design weaknesses and into ways of preventing core damage, which in most cases is the precursor of accidents leading to major radioactive releases with potential health and environmental consequences. In order to reduce the likelihood of occurrence of an accident one needs to design NPP systems for reliable operation and reliability can be engineered in NPP systems by:

- Selection of reliable parts/components
- Use of redundancy techniques with due consideration for minimizing common cause failures
- Design techniques such as derating so that the operating stress is below the specified strength of the parts/components
- Controlling the environmental conditions in which the NPP systems are operating
- Selection of passive systems where the actuation of systems depends upon physical phenomenon rather than electrical/pneumatic signals and devices
- Balance between the automation and operator interaction with the NPP systems for reducing operator errors.

1.2.2 Level 2 PSA

Level 2 PSA addresses the containment system and phenomenological responses, leading, together with Level 1 results, to the determination of containment release frequencies. It provides additional insights into the relative importance of accident sequences leading to core damage in terms of the severity of the radioactive releases they might cause, and insight into weaknesses in (and ways of improving) the mitigation and management of core damage accidents (e.g. severe accident management). To minimize the release of radioactive material, if accidents happen, the NPP design should ensure that

- NPP is established and maintained in safe sub-critical state
- Residual heat from reactor coolant system is removed
- The integrity of reactor coolant system and adequate supply of reactor coolant is maintained
- Containment integrity is maintained
- Reactor building pressure is maintained below the atmospheric pressure with the help of containment ventilation system
- All the opening of the containment are blocked with the help of containment isolation system.

The reliable operation of these systems is to minimize the release of radioactive material.

1.2.3 Level 3 PSA

Level 3 PSA addresses the off-site consequences, leading, together with the results of Level 2 analysis, to estimates of public injuries. It provides insights into the relative importance of accident prevention and mitigation measures expressed in terms of the adverse consequences for the health of the public, and the contamination of land, air, water and food provisions. In addition, it provides insights into the relative effectiveness of aspects of accident management related to emergency response planning. In order to minimize the population exposure if radioactive material is released the NPP design should take into consideration

- Construction of NPP in thin population area or in no population zone
- Procedures for emergency planning and preparedness
- Reliable communication and transportation facilities for speedy evacuation.

In constructing NPP in population zone efforts are required to minimize likelihood of occurrence of an accident and minimize the release of radioactive material.

PSA is performed for both internally initiated events and externally initiated events. In this section, Level 1 PSA will be discussed in detail for internally generated initiating events.

1.3 Level 1 PSA of NPPs

The first step in the Level-1 PSA studies is to identify the scope with respect to source of radioactivity, type of initiating events (IE) and operational state of the reactor. Once the Scope of PSA is identified the various tasks of PSA are mentioned below:

(i) Collection of information on design and operation of plant.
(ii) Initiating Event Identification and Grouping
(iii) Event Tree Analysis
(iv) System Modeling-Involves the following activities

  (a) Fault tree Development
  (b) Data Development and Parameter Estimation
  (c) Common Cause Failure Analysis
  (d) Human Reliability Analysis

(v) Core Damage Quantification and Accident Sequence Analysis
(vi) Uncertainty, Sensitivity and Importance Analyses.

Some of these steps are explained in the following subsections in detail. The plant logic diagram depicting the above process is shown in Fig. 1.

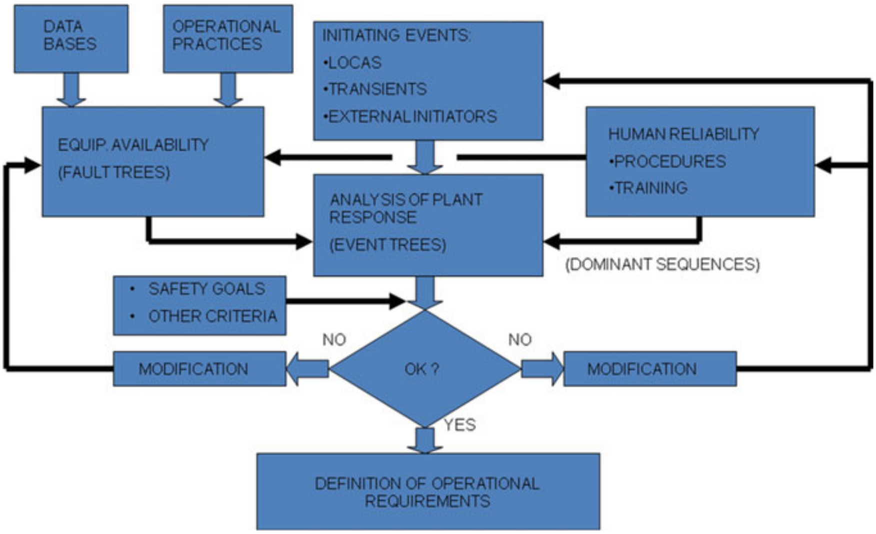


Fig. 1 Plant logic diagram

1.3.1 Identification of Initiating Events

An Initiating Event (IE) is an event that creates a disturbance in the plant and has the potential to lead to core damage depending on the successful operation or otherwise of the various mitigating systems in the plant

- There are two broad categories of Initiating Events:
  - *Loss of coolant accidents* (*LOCA*): Loss of coolant accidents is those accidents that may lead to draining of primary coolant because of isolation failures.
  - *Transient initiators*: Transients initiators are those initiators which affect the removal of decay heat and long term reactivity control.

The initial task of this analysis is to gather information from plant on design aspects and operation practices, which formed the basis for the development of plant models. There are several approaches that are followed for preparing the list of IEs, each approach having its own strengths and limitations. Engineering evaluation, Use of operational experience, Reference to previous lists etc. are few of them.

Once the Initiating events are identified then reactor shutdown and maintaining long term reactor sub-criticality, and decay heat removal are the safety functions necessary after their occurrence. The systems required for the proper functioning of the safety functions and those required for proper functioning of these front line systems are identified. Initiating Events are then grouped in such a way that all IEs in the same group essentially call for similar plant response and the same success criteria on front line systems. Some of the end-states in the event trees are fuel damages resulting from the postulated failures, for this the entire spectrum of fuel damage accidents has to be analysed and categorised (as per the performance of safety systems).

1.3.2 Plant Response Modeling: Event Tree Analysis

Event tree analysis is generally performed as follows: Event sequence modeling considers three basic functions that have to occur in succession for safe termination of the IE viz. reactor shut down, decay heat removal and long term reactivity control. To have a synthesised view of event sequences, small event tree, and large fault tree concept is used for event sequence modeling for various initiating events. In this concept the usual approach followed is that the front line system fault tree models include relevant support systems with suitable boundaries and human actions. Appropriate success criteria and boundary conditions are identified for various modes of front line system operation, which form the basis for their system modeling by fault tree method. For example, a simplified event tree for large Loss of Coolant Accident (LOCA) in a typical Pressurised Heavy Water Reactor (PHWR) is shown in Fig. 2. It has three pivotal events, viz.

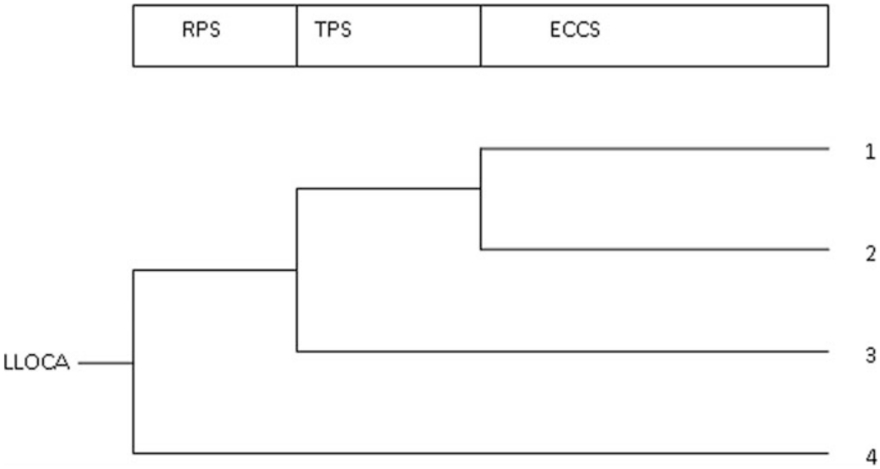


Fig. 2 A simplified event tree for large LOCA in a typical PHWR

- Reactor protection system.
- Total power supply system.
- Emergency core cooling system.

Theoretically event tree should have 8 paths, but it is having only 4 paths. This is because:

- RPS failure will directly have significant consequence irrespective of other events and
- ECCS is dependent on power supply.

The right side of event tree represents the end state that results from that sequence through the event tree. The end state can have healthy or accident consequences. To determine such consequence, through understanding of the system, operating experience, analyses of accidents (like thermal hydraulic or chemical reaction studies) is required.

1.3.3 System Reliability Modelling

Front line and support system modeling has been carried out using fault tree method. Salient features of these Fault Trees are immediate cause concept, detailed component modeling, use of combination of plant specific and generic component failure data for reliability parameter estimation, common cause failure analysis and incorporation of appropriate human error probabilities etc. The fault trees are deduced on the basis of design inputs available from sources like Design Manuals, Operating flow sheets including electrical, control and process drawings, single line diagrams, instrumentation schematics etc. To see the effect of any component failure in the overall risk, it is necessary that all the components and their logical relationships be available in the PSA model. Going down to the last component also allows effective treatment of common cause vulnerabilities.

The basic data required for a component appearing as a Basic Event in any system model is its unavailability which could be due to maintenance, test related problems or random failures of components, human errors etc. Reliability Parameters (for numerical values) considered are failure rate, repair time, test intervals, mission time, common cause component group, Human Error Probability (HEP), etc.

1.3.4 Common Cause Failure Analysis

Reliability of the system is enhanced by better design practice and selecting reliable components and further enhancement of reliability is achieved using redundancy technique. Redundancy means increase in volume, weight, cost and reduced maintainability. Moreover, 100% reliability cannot be achieved using redundancy technique. The limitation is dependent failures or common cause failures (CCF). Common Cause Failures can be defined as multiple failures which are a direct result of a common or shared root cause. The root cause may be design faults existing in redundant components catering to similar function, extreme environmental conditions (fire, flood, earthquake, lightning, etc.), or a human error (miscalibration, incorrect maintenance etc.).

For all other types of dependencies arising out of common design, manufacture, operation and maintenance and environment. Common Cause Failure analysis needs to be carried out with standard approaches such as Alpha factor model, Beta factor model etc. [4]. Most commonly used, beta factor model is a single parameter model; that is, it uses one parameter in addition to the total component failure probability to calculate the CCF probabilities. This model assumes that a constant fraction β of the component failure rate can be associated with common cause events shared by other components in that group. Another assumption is that whenever a common cause event occurs, all components within that common cause component group, are assumed to fail.

$$Q_{It} = (1 - \beta)Q_t$$
$$Q_m = \beta Q_t$$

This implies that

$$\beta = \frac{Q_m}{Q_{It} + Q_m}$$

where,

- Q_t, is the total failure probability of one component ($Q_t = Q_{It} + Q_m$)
- Q_{It}, is the independent failure probability of the single component
- Q_m, is the probability of basic event failure involving m specific components, m is the maximum number of components in a common cause group.

To generalize the equation, it can be written for m components involving failure of k components ($k \leq m$),

$$Q_{It} = \begin{cases} (1-\beta)Q_t & k = 1 \\ 0 & 2 \leq k < m \\ \beta Q_t & k = m \end{cases}$$

where,

Q_k is the probability of basic event involving k specific components.

Case study: Shutdown system based on shutoff rods as well as poison injection philosophy. For poison injection system, there are three poison tanks. For the successful functioning of the system, any two out of three poison tanks should be available. Find the system unavailability of Liquid Poison Injection System, if the poison tank unavailability (Q_t) is 1E−3 and β is taken as 10% for common cause failure model for liquid poison tanks in shutdown system.

For poison tank,

$$Q_m = \beta Q_t$$

$$Q_{It} = 9\text{E}{-4},\ Q_m = 1\text{E}{-4}$$

Considering 2/3 redundancy, as shown in Fig. 3, Liquid Poison Injection System unavailability from independent failures = 2.43E−6.

Total Liquid Poison Injection System unavailability = 1.02E−4.

1.3.5 Human Reliability Analysis

HRA has become an essential part of every Probabilistic Safety Assessment (PSA) and is used to identify human errors, quantify their likelihood in terms of Human Error Probabilities (HEPs) and correctly incorporate the HEPs in the assessment of risk. HRA in a PSA involves:

- Identifying the critical human interactions in the system and how they can fail.
- Quantifying their probabilities of failure in terms of HEPs.

Categorization of Human Interactions in PSA

Three categories of interactions can be defined to facilitate the incorporation of HRA into the PSA structure. The three categories are as follows:

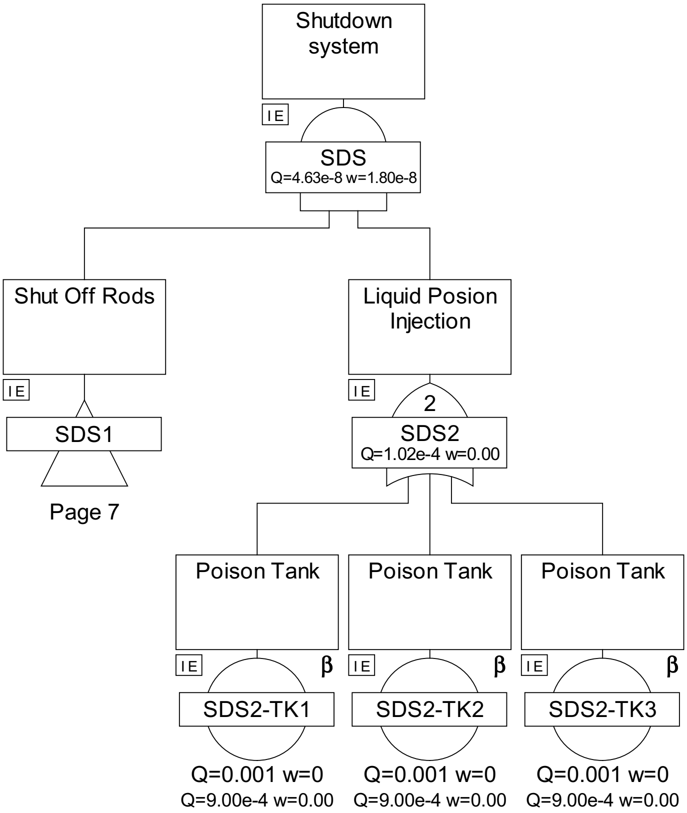


Fig. 3 Fault tree for shutdown system

- **Category A: Pre-Initiators**: These are activities prior to an Initiating Event (IE), related to maintenance, testing and calibration and intended to be positive. Any errors made in these interactions can lead to equipment or systems becoming unavailable when required post-fault. Pre-initiators consist of those actions associated with maintenance and testing, that degrade system availability. They may cause failure of a component/component group of may leave components in an inoperable condition. This unavailability is added to other failure contributions for components or systems, at the fault tree level. Recovery action for such human errors could follow error alarm, post–maintenance testing or post-maintenance inspection checks and may be modelled as applicable at the quantification stage. *These are independent of time and stress.*
- **Category B: Initiators**: Initiators are interactions carried out during normal operation, e.g. control room actions and normal maintenance, test or calibration actions. *Errors in these actions, either by themselves or in combination with other failures (other than human errors) can cause initiating events.* Most important are errors that not only precipitate an accident sequence but which

also concurrently cause failure of safety related systems, either front-line safety systems or support systems. Such 'common cause initiators' need to be specially emphasised.

- **Category C: Post-Initiators**: These are post-incident activities comprising the actions after an initiating event, performed with the intent to bring the plant back to normal safe and stable state. Errors in these interactions can occur while carrying out safety actions or there could be actions/errors that exacerbate the fault sequence. These human errors are associated with detection of the failure situation, diagnostics and subsequent actions for mitigation of Initiating Event. *These are the human actions required to be carried out in a limited time under high/moderate stress.*

Humans make errors due to a variety of causes. Some of the causes are internal to the individual (e.g. not knowing how to operate a particular equipment) and some are external to the individual (e.g. equipment controls not easily and comfortably accessible). The human's performance in a work situation is influenced by factors called Performance Shaping Factors (PSFs). The set of PSFs present in the work situation can greatly affect how safely or otherwise a system is operated. PSFs include factors like work environment quality of the Human Machine Interface (HMI) and quality of procedures and the training imparted. The identification of potential human errors is an important step in HRA. Errors, which alone or in conjunction with hardware/software failures, can lead to degraded system state are to be identified.

Human Error Quantification

After representing the human-error potential, the next step is to quantify the likelihood of errors involved and determine the overall effect of human error on system safety or reliability. Human reliability quantification techniques quantify human errors in terms of Human Error Probabilities (HEPs). HEP, which is measured as the ratio of the number of errors that occurred to the number of opportunities for the error to occur, is the metric of human reliability assessment. Recorded HEPs are relatively few in number. And also there is difficulty in estimating the opportunity for error in many tasks.

When HEP data are scarce, HRA resorts to quantification based on expert judgement or a combination of data and models that evaluate the effects of influences on human performance. The development of techniques of human reliability quantification has always been an area of significant activity. Important techniques are Technique for Human Error Rate Prediction (THERP) [5], Accident Sequence Evaluation Programme (ASEP) [6], Human Cognitive Reliability (HCR) [7], and newer techniques like Cognitive Reliability and Error Analysis Method (CREAM) and A Technique for Human Error Analysis (ATHEANA) [8]. CREAM and AHTEANA are second generation methods and are still not widely used in PSAs.

Human errors are modeled at Fault Tree level for pre initiators and for post initiators they are incorporated at Event Tree level in the Large FT and small ET approach.

1.3.6 Accident Sequence Analysis

Risk analysis is preferred due to its capability for quantification and thereby bringing out dominant risk contributors. In order to quantify, fault tree analysis and event tree analysis techniques are typically used for estimation of likelihood of selected incidents and evaluating frequencies. The process starts with development of event trees for these postulated events identified. Event tree modeling considers the procedure available to prevent the undesirable consequence in case an event happens, considering the role of safety functions in design. This activity comprises of identifying the systems involved in safety functions and probable human actions involved in event mitigation.

For PSA of NPP, major task is quantification of accident sequences that consist of an initiating event, along with mitigating system failures. Accident Sequences are identified using event tree methodology. Event tree analysis generates a large number of event sequences leading to different degrees of fuel damage. In view of the "defense in depth" approach applied in reactor design, an accident situation occurs when an initiating event is coupled with the unavailability of one or more safety systems. Unavailability can be obtained from fault trees for the particular systems. This leads to the evaluation of overall Core Damage Frequency, which in turn gives an indication of associated risk. Here risk is defined as follows:

$$Risk = \sum Accident\,Sequence\,Frequency \times Consequences\,All\,accident\,sequences$$

$$\begin{aligned}&Accident\,Sequence\,Frequency\,(ASF) = Initiating\,Event\,(IE)\,Frequency\\&\times\ Unavailability\,of\,one\,or\,more\,Engineered\,Safety\,systems/features\,(ESF)\\&associated\,with\,the\,IE\,for\,mitigation.\end{aligned}$$

Identifying accident sequence and estimating frequency of accident which include IE frequency estimation and Safety system unavailability estimation. For IE frequency estimation, either generic, plant specific data is used or fault tree analysis technique is used. For estimation of safety system unavailability, fault tree analysis technique is used. For estimating IE frequency, system unavailability and CDF, the following data is required

- Component failure data
- Human error data
- Common Cause Failure data
- Component maintenance data, etc.

In addition, vast amount of design information about reactor process and safety system is also required. The confidence in PSA results depend upon the input data.

In the figure below, on Class IV failure, plant shutdown function is performed by Shutdown system. On success of it, decay heat is removed by shutdown cooling system, which comes on auto. In case of shutdown system failure, fire water system can be injected manually. This is Type C, post initiator human action. Hence it is modeled in event tree, as shown in Fig. 4. Accordingly, consequences are identified based on safety analysis.

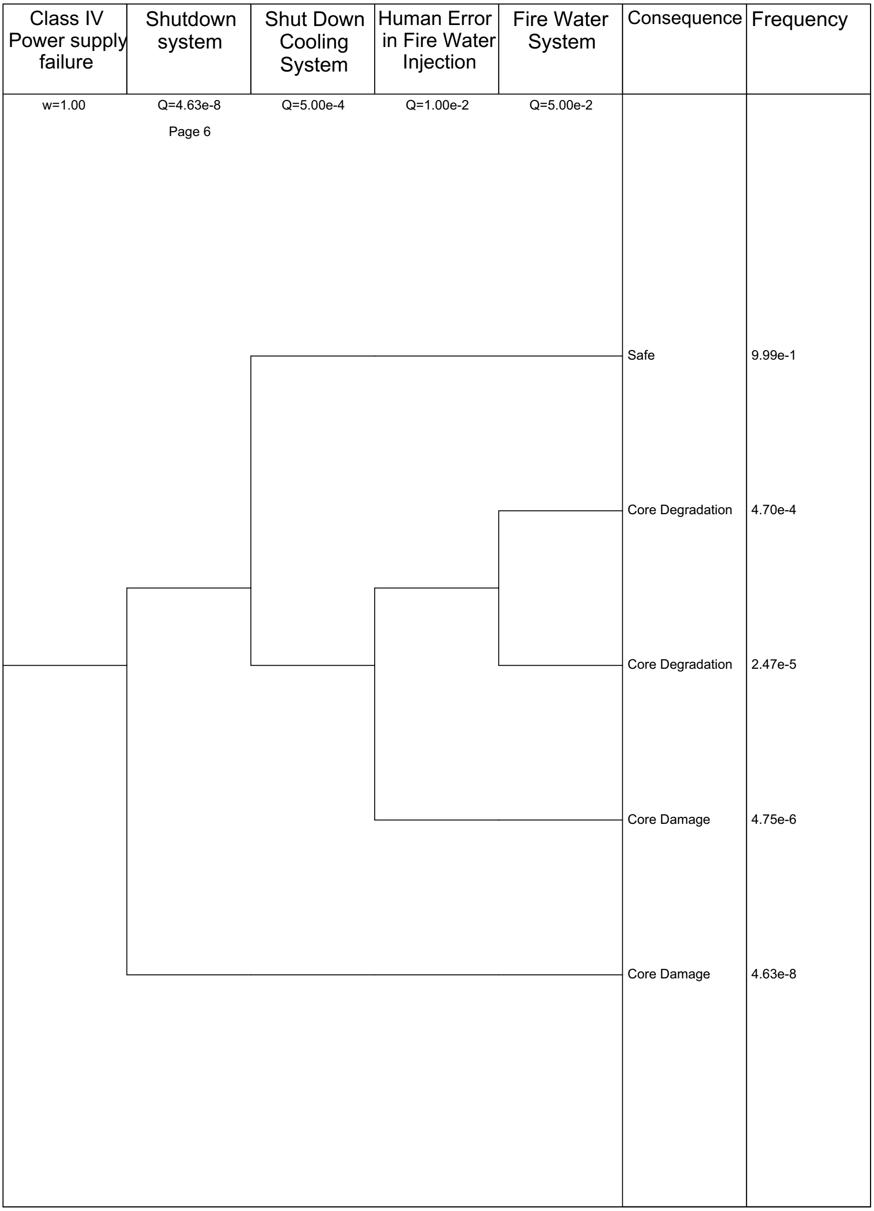


Fig. 4 Event tree for Class IV failure

In order to quantify the event tree, frequency of initiating event and unavailability of safety actions needs to be estimated. Class IV failure frequency is found from site/plant experience data. System availability of shutdown system, Shutdown cooling system and fire water system are found from fault tree analysis. For human error probability estimation, which is a high stress, time dependent action, models such as HCR, THERP, etc. are used.

1.3.7 Uncertainty Analysis

Parameter uncertainties are associated with the fundamental reliability parameters used in the PSA model. Model uncertainties are associated with incomplete understanding of certain processes or phenomena, introducing subjectivity in formulating modelling. Completeness uncertainties are not in itself an uncertainty, but a reflection of scope, limitations etc. and reflects an unanalyzed contribution, it is difficult (if not impossible) to estimate its magnitude.

The Parameter uncertainty, which arises from the quantification of the frequencies and probabilities of the individual Basic Events needs to be addressed in the PSA studies. Importance and Sensitivity Analysis are carried out for all basic events, CCF Groups, various frontline and support systems and for all dominant event sequences for ranking the components to prioritise corrective measures.

1.4 PSA Application in Safety Issues

Risk Informed technology is being extensively applied in various areas as a support tool for routine as well as in critical decision making. Risk Informed techniques are structured to improve the testing and maintenance of highly safety significant components and to reduce unnecessary testing resource allocation towards low-safety significant components. PSA results provide a technical basis for ranking components/systems with respect to their contribution towards Risk. Such ranking can be effectively employed for obtaining solutions for various issues encountered by Regulatory bodies as well as by Nuclear Power Plant Operators. Some important applications of PSA towards Safety Issues are discussed in forthcoming sections.

1.4.1 Probabilistic Precursor Analysis

PSA based analysis of operational events or of precursor analysis answers two basic questions: (a) How could a precursor event have degenerated into an accident with more serious consequences? (b) Is it possible to determine and measure what separates a precursor event from a potential accident with more serious consequences? Thus, the analysis contains a qualitative and a quantitative element. The minimal cutsets provide the Qualitative element to Precursor by identifying the combination of component failures required for the core damage type of accident to happen. ***In addition, PSA helps in providing a Quantitative element to the precursor analysis,*** **viz**., measuring the severity of the event.

Some of the event severity measures considered are—The conditional core damage probability (CCDP). For an initiating event, the CCDP is the conditional probability of core damage given the event. For a condition event, the CCDP is the increase of the core damage probability due to the event (increase in ICDF multiplied by the duration of the condition).

The instantaneous core damage frequency (ICDF), which applies only to condition-type events, is used as an intermediate step in the calculation of the CCDP.

The conditional probability that an operational event would progress to accidents with unacceptable consequences is more widely accepted severity measure. Based on this information, events can be ranked according to their risk significance. Moreover it can be used to prioritize which weaknesses should be handled first, and to assess the level of safety of the plant.

Basically there are two types of precursor events:

(i) The precursor event represents a transient which interrupts normal operation of the plant, thus there is a real effect on plant operation. In this case the event can be easily related to an initiating event of the PSA (if modelled) and the accident scenarios affected by the event are those developing from this initiating event.

When an IE has occurred, the core damage frequency f_{IE} is calculated from the event tree corresponding to the IE, and the CCDP is calculated as

$$CCDP = f_{\mathrm{IE}}/\lambda_{\mathrm{IE}},$$

with λ_{IE} the frequency of the IE.

(ii) The precursor event involves the unavailability or a degradation of equipment or systems without an immediate impact on plant operation. If the precursor event is related to one (or several) safety functions, a systematic survey of the principal scenarios on which the precursor event impacts needs to be done. First, all the initiators which require the affected safety function(s) need to be identified. In the event scenarios or sequences developing from these initiating events (Event Trees) only the scenarios which entail the precursor event are retained.

Preferably the computerized PSA database is used for this purpose to ensure that the search and identification process is exhaustive.

Precursor events which entail both, an initiating event and equipment or system unavailability, are also possible and both types of impacts need to be included in the subsequent analysis in a combined manner.

The primary result is the ***conditional probability for core damage***, given that the precursor event has happened.

The CCDP value is calculated as:

$$CCDP = T_{\text{event}} \times \left(CDF_{\text{event}} - CDF_{\text{base}}\right)/A$$

with A the duration of power operation per year, T_{event} the duration of the operational event (h), CDF_{event} the core melt frequency during the event (1/y), and CDF_{base} the base value of core frequency during power operation (1/y).

The main results of precursor investigations are the conditional probabilities for Core Damage from PSA model given that operational event has happened. As a numerical threshold for judging the significance of operational events based on a conservative estimate of the conditional core damage probability a value of 10^{-6} is widely accepted and used. Multiplying the conditional probability of the precursor event j with the frequency, i.e. one event within the observation time in reactor years, and summing up all precursor events within the observation time yields:

$$\lambda = \sum_{j} \frac{CCDP_j}{Observation\, time} \tag{3}$$

where j represents the operational events identified for precursor analysis.

λ is an estimator for the unacceptable consequences, typically either core damage frequency or beyond design basis frequency. The estimator is called ***core damage index***, beyond design basis index, or simply safety or risk index.

The major advantages of this approach are the strong potential for augmenting event analysis which is currently carried out purely on deterministic basis. From the observations it is found that there is slight discrepancy between CCDP values and INES scale associated to an event. Also, the risk index gives an indication about the safety culture followed in plant and can be used as a metric for comparing between various plants.

1.4.2 Probabilistic Vital Area Identification

Identification of vital areas in a facility involves assessing the facility and the locations, whose sabotage can result in undesirable (radiological) consequences. Probabilistic Safety Assessment (PSA) technique can find the component failures leading to core damage (a surrogate for radiological consequence) in a systematic manner, which can be extended to identification of vital areas. The procedure for the generation of location sets (set of locations whose sabotage can lead to possible core damage) and protection sets (set of locations that must be protected to prevent possible core damage). In addition, measures such as ***vulnerability and protectability*** have been introduced, which can be used to rank location sets and protection sets [9].

Vital area identification is helpful, only if, analysis can come up with protection sets. A protection sets represent locations which, when protected, will prevent an adversary from accomplishing sabotage. In order to find the protection set, it is required to construct the location fault tree from the minimal location sets. Following logics are employed to convert location set to location fault tree.

(a) All cut sets are combined using AND gate
(b) Within a cutset, the locations are connected using OR gate.

Protection sets are the minimal cutsets obtained from location fault tree.

Thus the sabotage logic model, (For e.g. the core damage logic model for Nuclear Power Plants, large toxic release model for chemical plants, etc.) is then analyzed to identify the target sets or vital area sets (combinations of areas the adversary must visit to cause radiological sabotage) and the candidate protection sets (combinations of areas that must be protected against adversary access to prevent radiological sabotage).

1.5 Summary

PSA presents an Integrated Picture of the Safety of NPP which encompasses Design, Operational Practices, Component Reliability, Dependencies and Human Reliability. It also helps in identifying predominant contributors to possible Severe Core Damage in terms of Component Failures and Human actions. Also, it identifies any weak-links or imbalances affecting the Safety of the plant with reference to Components/Human actions, which could be improved. In short, PSA of nuclear power plant is an effective technique to minimise accident frequency and consequence by better design technique in power plant system and containment, to develop operational maintenance and accident management procedure and emergency preparedness procedure.

2 Probabilistic Safety Assessment of Non-reactor Nuclear Facilities

2.1 Introduction

The operation of Non Reactor Nuclear Facility (NRNF) differs significantly from Nuclear Power Plants (NPPs). These facilities employ a greater diversity of technologies and processes. Fissile materials, wastes, radiation sources are handled, processed, treated and stored throughout the nuclear installations, in contrast to reactors, where the bulk of the nuclear materials are located in the reactor core and fuel storage areas. Greater reliance is put on the operators, not only to run the facilities during normal operation, but also to respond to fault and accident conditions. Chemical processes, if not managed properly, may lead to inadvertent release of toxic chemicals or radioactive substances. Similar to NPP, facilities also needs to keep the radiation exposure from nuclear facilities to members of the public and workers as low as reasonably achievable (ALARA) during normal operational states (certainly below the limits set by the regulatory bodies) and in the event of accident. Another type of NRNF is Accelerator facilities, which have emerged as powerful tools for research in physics, chemical sciences, material sciences, etc. They are associated with hazards from radiation sources (bremsstrahlung radiation and neutrons), energy sources, hazardous materials etc. In order to adhere to the safety goal, carrying out safety analysis has become almost mandatory for all nuclear facilities.

2.2 *Steps in PSA for Nuclear Facility*

The major steps of PSA for nuclear facility are mentioned below:

- System description
- Hazard identification
- Incident enumeration
- Accident Sequence Quantification
- Risk estimation.

These steps are explained in forthcoming subsections.

2.2.1 System Description

System description involves collection of information on design and operation of plant, i.e., compilation of all technical and human information needed for the analysis (including reliability data). Information was assembled using sources such as safety analysis reports, design manuals, operating practices etc.

2.2.2 Hazard Identification

This is a critical step in risk analysis, a hazard omitted at this stage is a hazard which is not analysed. Typically nuclear facilities, such as accelerator houses potential hazards, like

- Radiation
- Heat load
- Electrical
- Ozone and
- Fire.

For electron accelerator, hazards associated with ionizing radiation arise during several aspects of operation: loss of electrons from the beam at various stages of acceleration; loss of electrons from the beam circulating in the storage ring; and synchrotron radiation emanating from bending magnets and insertion devices located around the storage ring.

2.2.3 Incident Enumeration

Preparation of list of postulated events is a very important task in risk analysis, which needs completeness in identification and tabulation of all incidents without any relevance to their importance or to the initiating event. The approach used for preparation of postulated events is based on:

- Precursor review
- Engineering evaluation
- Use of operational experience.

Since there are no standards/documents listing postulated events from an accelerator and they can vary with design, these approaches may not be conclusive. However, elaborate discussions needs to be undertaken to consider events to the extent possible.

For accelerator, typically initiating events from beam lines are analysed which leads to undesirable consequences such as high radiation due to inadvertent beam dump, Personal exposure in experimental hutch due to failure in safety barriers, etc. [10]. Various events such as ‘Loss of target cooling’, ‘Vacuum degradation due to sputter ion pump failure’ can result in beam dump. Similarly, Personal exposure can happen due to Inadvertent entry during experiment, Spurious opening of safety shutter, etc.

2.2.4 Accident Sequence Quantification

For all Postulated Initiating Events, event progression is modelled using event trees. In case of accelerator, the safety function can result either in tripping beam or closing the safety shutters, hence consequence is analysed in terms of dose received from beam dump or personnel exposure. For all PIEs, consequence estimation is carried out to determine the potential damage from radiation (dose assessment to public, accidental exposure, etc.).

A typical event tree for “Spurious opening of Safety Shutter” (SOSS) is given below. This event can happen in experimental hutch, while preparation of experiment is being carried out. Normally, the safety shutter will be in closed condition. Postulated initiating event considered in this case is ‘Spurious opening of Safety Shutter’, which can have undesirable consequence, if beam is ON and Area is occupied. Frequency of initiating event can be found using fault tree approach enumerating all the causes and their failure rates. Similarly, Probability of conditions such as 'beam is ON' and 'Area is occupied' can be found from plant experience.

From the event tree shown in Fig. 5, frequency for undesirable consequence such as Personnel exposure can be found. Dose assessment, during this event, are considered in consequence estimation.

2.2.5 Risk Estimation

Once likelihood or frequency of incident is estimated along with the specified consequences, it is required to combine them in a meaningful fashion to provide a measure of risk. Many measures of risk have been proposed and are in use, each providing a different view of a particular situation or aspect. Among these measures, perhaps most commonly used ones are those of individual risk and societal risk.

For accelerator like facility, it is appropriate to devise an F-N curve with consequences expressed in released activity in terms of curies (or Becquerel's) of various radionuclides, health effects like early fatalities and latent cancers, and radiation doses (rems or sieverts). NUREG 1860 [11], has proposed an F-C curve in terms of radiation doses, is popularly used for PSA of NRNF, as shown in Fig. 6.

F-C curve, as per NUREG 1860, is applied for communicating the risk from the events identified from the accelerator. Figure 7 shows the typical F-C curve obtained for electron beam accelerator.

It can be found that 'SOSS' falls in the Acceptable region, which ensures the safe regime of Accelerator Fig. 8.

3 Probabilistic Safety Assessment of Non–nuclear Facilities

3.1 Introduction

PSA in non-nuclear facility such as chemical/industrial facility is commonly referred to as Quantitative Risk Assessment (QRA). The QRA methodology has evolved since the early 1980s from its roots in the nuclear, aerospace and electronics industries. The most extensive use of probabilistic risk analysis has been in the nuclear industry. The QRA has since then moved to other sectors, including the Process Industry. The QRA can be defined as the analytical process with which the hazards are identified and the probability of a damage occurring following occurrence of any of the identified hazards is evaluated. From this analysis, the calculated risk is then assessed with reference to suitable tolerability criteria. QRA has a number of specific features:

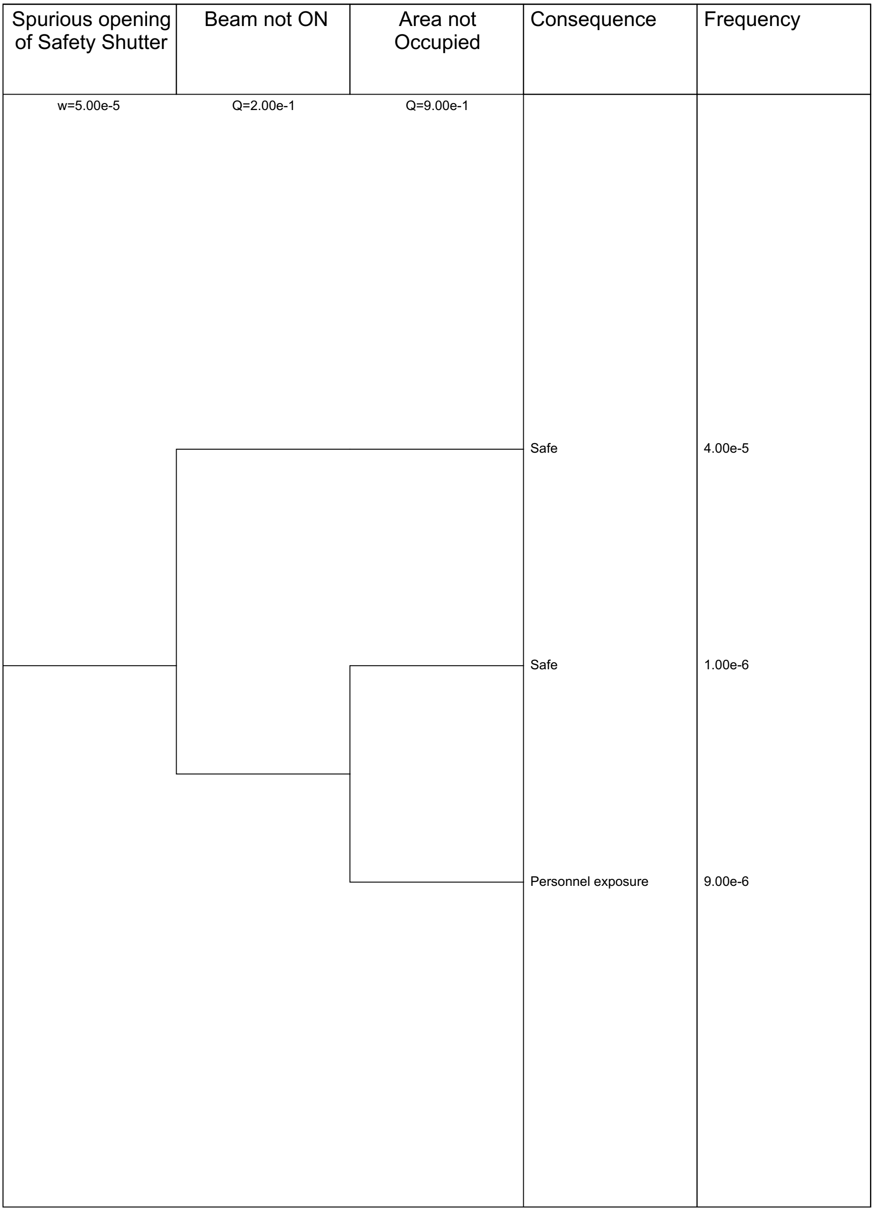


Fig. 5 Event tree for 'spurious opening of safety shutter' (SOSS)

- Chemical reactions may be involved
- Processes are generally not standardized
- Many different chemicals are used
- Material properties may be subject to greater uncertainty

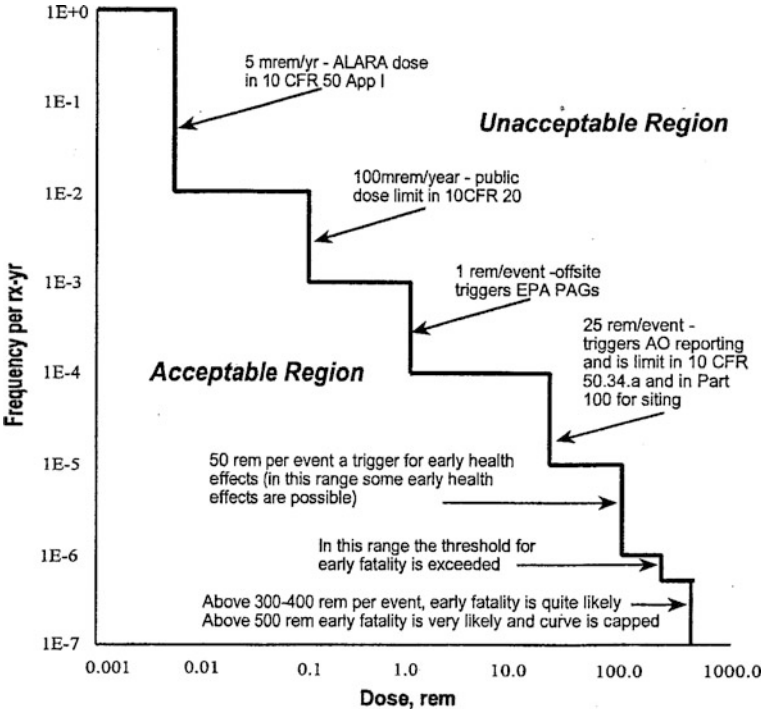


Fig. 6 F-C curve from NUREG 1860

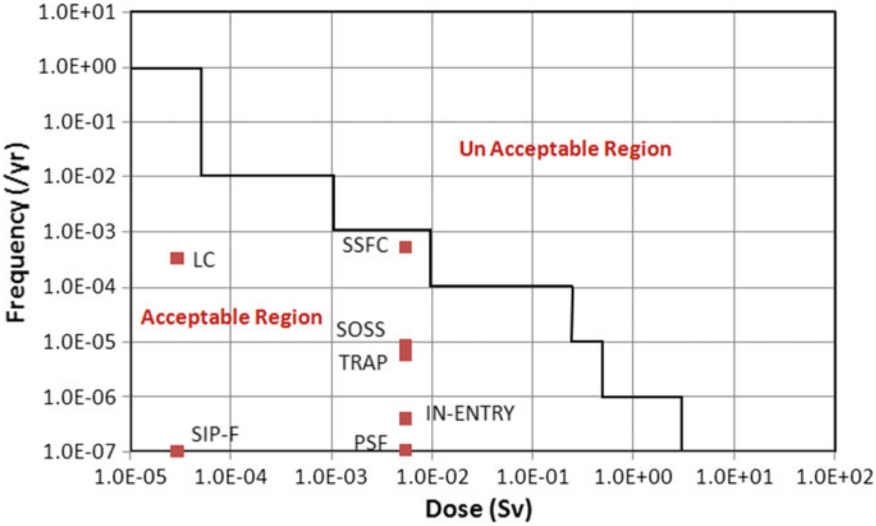


Fig. 7 Frequency versus dose curve for experimental hutch

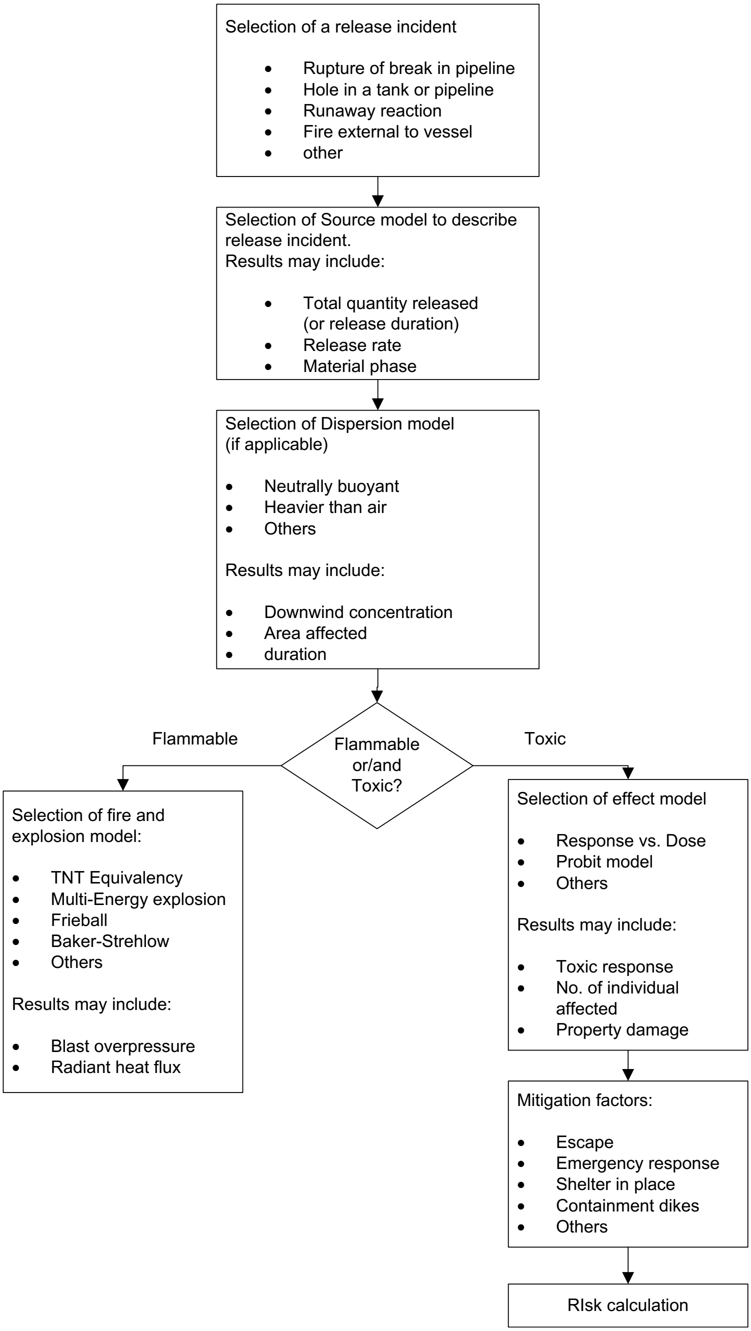


Fig. 8 Consequence analysis from volatile hazardous material release

- Parameters, such as plant type, plant age, location of surrounding population
- Degree of automation and equipment type, vary widely
- Multiple impacts, such as fire, explosion, toxicity, and environmental contamination.

Acute, rather than chronic, hazards are the principal concern of QRA. This places the emphasis on rare but potentially catastrophic events. The risk (*a measure of safety*) in general for industrial facility is defined as:

$$\textbf{Risk} = \textbf{Probability of an accident} * \textbf{Consequences in terms of exposure to toxic material}$$

In this session, QRA will be referred as PSA.

3.2 Steps in PSA for Chemical Facility

The major steps of PSA for chemical facility are mentioned below:

- Hazard identification
- Incident frequency estimation
- Consequence estimation
- Risk estimation.

These steps are explained in forthcoming subsections.

3.2.1 Hazard Identification

The correct identification of Hazards is the first essential step for a Risk Analysis. Various techniques can be adopted depending on the level of information available. One of the most widely used techniques for Process plant hazard identification is the HAZOP analysis. A HAZOP study is a structured analysis of a system, process or operation, carried out by a multi-disciplinary team. The team proceeds on a line-by-line or stage-by-stage examination of a firm design for the process or operation. The team concentrates on those deviations that could lead to potential hazards to safety, health or the environment. This is done by using a set of guidewords in combination with the system parameters to seek meaningful deviations' from the design intention. A meaningful deviation is one that is physically possible—for example, no flow, high pressure or reverse reaction.

3.2.2 Incident Enumeration

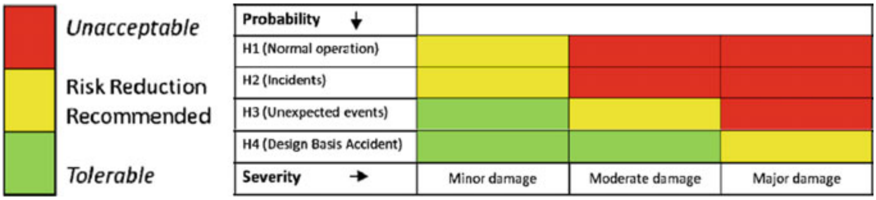
HAZOP forms starting point of incident enumeration. In addition to the identification of hazards, it is common practice for the team to search for potential operating problems. These may concern security, human factors, quality, financial loss or design defects. Where causes of a deviation are found, the team evaluates the consequences using experience and judgment. If the existing safeguards are deemed inadequate, the team recommends an action for change or calls for further investigation of the problem. In summary, approaches used for preparation of postulated events are based on:

(i) HAZOP review
(ii) Engineering evaluation
(iii) Use of operational experience.

Incident enumeration is closely linked with hazard identification and has to be dealt in total. For example, chlorine gas is a ‘hazard’ while its unplanned emission through a faulty valve is an ‘incident’. Once postulated initiating event list is finalized, event tree modeling is performed to understand procedures available to prevent the undesirable consequence in case an event happens. In chemical facility, the major action is focused on preventing toxic exposure. This activity comprises of identifying the systems involved in safety functions and probable human actions involved in event mitigation.

3.2.3 Consequence Estimation

Consequence estimation is the methodology used to determine the potential damage or harm from specific incidents and is closely linked with hazard under consideration. The first step of the Consequence analysis is the calculation of the characteristics of the release of the material: the Source Model. Accidents usually begin with the loss of containment of material from the process. The material has hazardous properties, which might include toxic properties and energy content. Typical incidents might include the rupture or break of a pipeline, a hole in a tank or pipe, runaway reaction, fire external to the vessel, etc. Once the incident is known, source models are selected to describe how materials are discharged from the process. The source model provides a description of the rate of discharge, the total quantity discharged (or total time of discharge), and the state of the discharge—solid, liquid, vapor, or a combination. A dispersion model is subsequently used to describe how the material is transported downwind and dispersed to some concentration levels. For flammable releases, fire and explosion models convert the source model information on the release into energy hazard potentials such as thermal radiation and explosion overpressures.



🟥	Unacceptable
🟨	Risk Reduction Recommended
🟩	Tolerable

Probability ↓			
H1 (Normal operation)	🟨	🟥	🟥
H2 (Incidents)	🟨	🟥	🟥
H3 (Unexpected events)	🟩	🟨	🟥
H4 (Design Basis Accident)	🟩	🟩	🟨
Severity →	Minor damage	Moderate damage	Major damage

Fig. 9 Qualitative risk matrix

3.2.4 Risk Estimation

Categorization of risk involves assessment of risk taking into consideration the probability and severity of consequence. There are qualitative and quantitative methods available for risk categorization.

Qualitative risk ranking schemes

In typical qualitative risk assessment approach risk matrix is developed as shown in Fig. 9. Three levels of risk are defined; "Unacceptable", "Risk Reduction Recommended" and "Tolerable". Unacceptable risks require risk reducing measures in order for the suggested design to be accepted. Risks Reduction Recommended require a demonstration that the suggested barriers are as effective as reasonably can be achieved considering alternatives and additions. Tolerable risks require no additional barriers, but need to be monitored, for example when design changes, to be kept at a low level.

Quantitative risk ranking schemes

The risk matrix is depiction of the frequency and consequences. Quantitative treatment can also be extended to risk matrix. Typical scheme of risk indexing is shown in Fig. 10. The probability values can be high ($<10^{-1}$ per year), medium (10^{-2} to 10^{-1}), low (10^{-4} to 10^{-2}) or extremely low (10^{-6} to 10^{-4}). The consequences are categorized as high to extremely low based on whether the incident has serious impact on off-site and on-site.

3.3 Risk Based Inspection for Chemical Facility

Last decade saw a trend where life management programmes are globally moving from prescriptive/time-based towards risk- based decision making. Risk analysis finds use/application in decision making, for operation, maintenance and regulatory activities. This methodology has been applied in planning maintenance activities such as testing time, repair time, inspection interval etc. When this is applied to inspection planning, it is termed as Risk based inspection. Risk Based Inspection

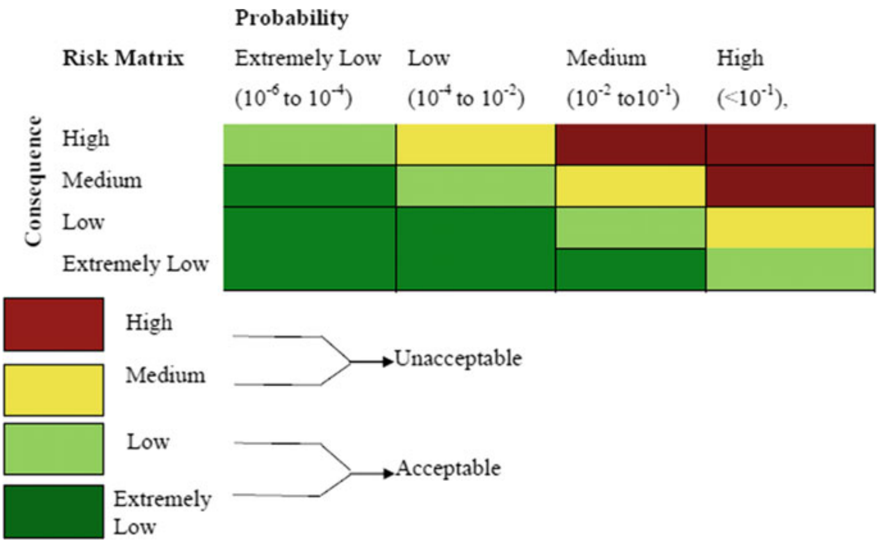


Fig. 10 Risk indexing

(RBI) is a method for using risk as a basis for prioritizing and managing the efforts in an inspection program. Risk Based Inspection focuses the utilization of risk quantification in formulating an In-Service Inspection (ISI) plan thereby emphasizing the importance of surveillance and maintenance activities on plant risk. RBI would be able to establish an effective structural integrity management programme, which reduces plant down time, industry and regulatory burdens, and continue to maintain plant safety. For applying the frame work of Risk Based Inspection, it is required to estimate ***likelihood or probability of failure*** (***PoF***) of components in process plant and their ***consequence*** (***CoF***), in terms of damage to the equipment and impact of toxic release to public.

Probability of Failure (PoF) of a component can be estimated from operating experience data/stress-strength models/expert judgment. Service Data Analysis based on operating experience is one of the popularly employed method used for this purpose. Data bases such as OREDA 2002 [12] are the result of various collaborative efforts taken towards methodical collection of operating experience information, which can be termed as generic data base. Consequence of Failure (CoF) estimation, looks into damage as well as toxic impact analysis. Consequence analysis can be performed either in a qualitative manner or detailed quantitative analysis. API 581, Base Resource Document for Risk based Inspection [13], may be used, which provides factors for damage and toxic consequence. After determining the PoF and CoF category, it needs to be applied to Risk matrix to establish the inspection category [14].

4 Concluding Remarks

While doing Probabilistic Safety Assessment, major challenge is in ensuring the correctness and completeness of initiating events possible from the industry. Probability of these events are depend on industry specific, since it needs to consider the environment, test and maintenance practices, safety culture prevailing etc. However, while conducting such analysis at the design, falls back on available information from generic source. It is recommended to have a proper data collection process to improve the predicted failure rates to be made realistic to the extent possible. The consequence analysis finally gives us the individual and collective exposures to hazardous material, number of health effects (both fatal and non-fatal), and costs of disruption. These consequences can be mitigated by countermeasures and the effect of countermeasures on the exposure also accounted in the consequence analysis codes. The analysis tool will help decision makers to estimate numbers of people and areas affected by emergency countermeasures. The probabilistic approach will give statistical results like minimum, maximum, xth percentile number of people exposed to a threshold dose/hazards or areas to be evacuated. Hence Probabilistic Safety Assessment is an essential tool for ensuring the safety of any type of facility.

References

1. Fullwood R, Hall RE (1988) Probabilistic risk assessment in the nuclear power plant industry: fundamental application. Pergamon Press, Brookhaven National Laboratory, New York, USA
2. Reactor Safety Study, WASH-1400, NUREG-75/014, United States Nuclear Regulatory Commission (1975)
3. NUREG-2300, PSA Procedures Guide (1983)
4. EPRI NP-5613, Procedures for treating common cause failures in safety and reliability studies, vol. 1, NUREG/CR-4780 (1988)
5. Swain D, Guttmann HE (1983) Handbook of human reliability analysis with emphasis on nuclear power plant applications. NUREG/CR-1278. US Nuclear Regulatory Commission, Washington DC
6. Swain AD (1987) Accident sequence evaluation program human reliability analysis procedure. NUREG/CR-4772. US Nuclear Regulatory Commission, Washington DC
7. Case study on the use of PSA methods: human reliability analysis. IAEA-TECDOC-592 (1991)
8. Forester J et al (2007) ATHEANA User's Guide. NUREG-1880. US Nuclear Regulatory Commission, Washington DC
9. Vinod G, Sanyasi Rao VVS, Ghosh AK, Kushwaha HS (2012) PSA based vulnerability and protectability analysis for NPPs. Ann Nucl Energy 50:232–237
10. Sanyasi Rao VVS, Vinod G, Sarkar PK, Vaze KK (2012) Application of PSA techniques to synchrotron radiation sources. Indian J Pure Appl Phys 50:776–781
11. NUREG 1860 Feasibility studies for a risk-informed and performance-based regulatory structure for future plant licensing
12. OREDA (2002) Offshore reliability data base

13. API (1998) API Publication 581, Base Resource Documentation—Risk-Based Inspection. American Petroleum Institute
14. Vinod G, Sharma PK, Santosh TV, Hari Prasad M, Vaze KK (2014) New approach for risk based inspection of H2S based process plants. Ann Nucl Energy 66:13–19

Dr. Gopika Vinod joined Reactor Safety Division of Bhabha Atomic Research Centre as a Scientific Officer from 37th batch of Training School after completing her graduation in Computer Engineering. She received her doctoral degree in Reliability Engineering from Indian Institute of Technology, Bombay and also been Post-Doctoral Fellow at Steinbies Advanced Risk Technologies, Germany. She is a recipient of DAE Young Engineer Award 2007. She has been to visiting scientist at Brookhaven National Laboratory. Currently she is heading the Probabilistic Safety Section of Reactor Safety Division of BARC. She also holds the position of Faculty with Homi Bhabha National Institute. She has been actively involved in reliability, safety, and risk analysis of Indian nuclear power plants. She has worked on the development of reliability-based operator support systems such as risk monitor, symptom-based diagnostic system, for Indian nuclear power plants. Her other areas of research activities include risk-informed in-service inspection, reliability of computer-based systems, dynamic reliability analysis, etc.