Application of PSA techniques to synchrotron radiation source facilities

V V S Sanyasi Rao, Gopika Vinod, P K Sarkar1 & K K Vaze
Reactor Design and Development Group,1 Health Physics Division, Bhabha Atomic Research Centre, Mumbai 400 085

*E-mail: sanyasirao.vvs@gmail.com, vgopika@barc.gov.in
Received 23 August 2012; accepted 28 September 2012

Synchrotron radiation sources are increasingly being used in research and medical applications. Various instances of overexposure in these facilities have been reported in literature. These instances have led to the investigation of the risks associated with them with a view to minimize the risks and thereby, increasing the level of safety. In nuclear industry, Probabilistic Safety Assessment (PSA) methods are widely used to assess the risk from nuclear power plants. PSA presents a systematic methodology to evaluate the likelihood of various accident scenarios and their possible consequences using fault/event tree techniques. It is proposed to extend similar approach to analyze the risk associated with synchrotron radiation sources.

Keywords: Probabilistic safety assessment, Nuclear power plant, Accelerator, Risk

1 Introduction

Main aim of nuclear safety is to keep radiation exposure from nuclear facilities to members of the public and workers as low as reasonably achievable (ALARA) during normal operational states and in the event of accidents. International definition of safety is capacity of unit not to lose or let occur endangering of person for specified time and conditions. There is a difference between reliability and safety. Reliability talks about only probability of success of the system while safety is essential when system is in operation or in failed/non operation state.

Safety analysis of facility is aimed at the calculation of risk due to the operation of facility and its comparison with other natural and industrial risks. It is based on both on deterministic and probabilistic safety analyses (PSA). In the deterministic safety analysis, design basis accidents are considered and it is shown that such accidents do not result in radiation doses/ risks that are above regulatory limits. In case certain accidents result in doses above regulatory limits, design changes are incorporated to ensure that the doses are below the limits. In contrast, probabilistic safety analysis (PSA) considers all possible accident scenarios and their quantification in terms of plant damage frequency and consequences.

The risk (a measure of safety) in general for Nuclear Power Plant (NPP) is defined as:
Risk= Probability of an accident × Consequences due to exposure to radioactive material released.

The risk can be minimized by minimizing the accident frequency or its consequences or both.

2 Probabilistic Safety Analysis of NPPs

Probabilistic Safety Assessment (PSA) of nuclear reactors, essentially aims at identifying the events and their combination(s) that can lead to severe accidents, assessing the probability of occurrence of each combination and evaluating the consequences. This helps to rank the systems and components in terms of their risk significance.

PSA methodology integrates information on plant design, component reliability, operating practices and history, human behaviour, Postulated Initiating Events (PIEs), accident sequences and potential environmental and health effects. This helps in focusing on issues like deficiencies and plant vulnerabilities, risk contributors, sensitivity of governing parameters and uncertainties of numerical results. A full scope PSA is performed in three levels:

(1) Level 1 PSA is the starting block of probabilistic safety assessment methodology that arrives at Core Damage Frequency.

(2) Level 2 PSA taking inputs from Level 1 PSA results quantifies the magnitude and frequency of radioactive release to the environment following core damage progression and containment failure.

(3) Level 3 PSA taking inputs from Level 2 PSA results, analyses the transport of radionuclides through the environment, the contamination of land, air, water and foodstuffs due to dispersion of radionuclides and assesses the public health and economic consequences of the accident. Level 1 PSA is discussed in detail and it involves following steps:
In view of the “defense in depth” approach applied in reactor design, an accident situation occurs when occurrence of an initiating event is coupled with unavailability of one or more ESFs. It leads to evaluation of overall Core Damage Frequency.

**Risk or Core Damage Frequency (CDF)**

\[
\text{CDF} = \sum_{\text{All IEs}} \text{Frequency of IE}_i 
\]

\[
\times \sum_{k=\text{All AS for } i} \left( \prod_{j} \text{unavailability of SS}_j \right) \quad \ldots \ (1)
\]

Here, \( j \) extends over all the safety systems (SSs) that are needed to operate in a given accident sequence (AS), \( k \), initiated by the IE \( i \).

### 3 Uses of PSA Studies

Whenever any modifications or change of configuration are required to be incorporated in an operating plant, PSA studies can assist Plant operators as well as regulators to assess the risk and ensure that plant is in the prescribed safe domain. Various such decision making issues encountered are in operations, maintenance, In-Service Inspection. Safety guidelines/goals/targets for various parameters, such as unavailability of a system, conditional core damage probability, allowed down time for component or system specified by regulatory body, can be compared with actual values observed in the plant and decisions regarding various issues can be taken by the plant management. In addition, the measured CDF, can be used for putting in proper perspective the concerned plant in relation to other NPPs.

### 4 Synchrotron Radiation Sources

Synchrotron Radiation Sources contain charged particle generators, injectors, boosters, storage rings and beam lines in experimental hutches. Electromagnetic radiations generated by bending the path of electrons moving at speeds closer to light are called synchrotron radiation. Experimental hutches are used by experimenters for conducting research in the area of physical, chemical and biological sciences. Usually, these hutches are provided with interlock systems. The loss of high-energy electrons during operation of the accelerators and storage ring generates bremsstrahlung and neutron radiation for which shielding must be provided. Exposure of personnel to this radiation is prevented by permanent shielding and the Access Control Interlock System (ACIS) for the accelerator and beam-line enclosures. Radiation monitors are located outside the experimental hutches which continuously monitor the radiation levels and aid the operating staff to take appropriate decisions whenever the radiation levels exceed some preset values.

### 5 PSA of Synchrotron Radiation Sources

In accelerators, the radiation hazard diminishes practically whenever the machine is switched off. However, maintenance of any equipment within the storage rings involves taking certain precautions as activation products may be present in areas where beam slits/beam dumps are present. The energy of the Bremsstrahlung radiation can extend up to the energy of the particle in the storage ring. Since thick shielding is provided, under normal operating conditions, the chances of receiving high radiation dose are low.

Even though these facilities have emerged as powerful tools for research, they are associated with hazards from radiation sources. Various instances of overexposure in these facilities have been reported in literature like Therac-25 etc. These instances have led to the investigation of the risks associated with them with a view to minimize the risks and thereby increasing the level of safety. The likely types of failures and their consequences for the system as a whole should be taken into account. Examples include: (a) Loss of access control; (b) Malfunctions and failures of structures, systems and components; (c) Electrical distribution faults, from localized faults to complete loss of external energy sources; (d) Failure resulting from external causes; (e) Failure of personnel to observe proper, safe procedures; (f) Breakdown of procedures for preventing access to the facility by unauthorized persons; (g) Breakdown of administrative procedures leading to unsafe practices.
In case of accelerator facility, hazard analysis needs to concentrate to areas such as injector, synchrotron, transfer lines and storage rings. For these facilities, the risk of accidental exposures can be kept to a minimum by proper design and construction, with specific attention to shielding, interlocks, and a good radiation protection programme with proper training and access control. It is, therefore, essential that adequate radiation safety measures should be taken according to the objectives laid down in documents such as Basic Safety Standards of IAEA.

Another hazard related with this type of facilities, is the ozone production, with interactions between air and ionized radiation. Typical limit of concentration on ozone considered in hazard analysis is less than 0.1 ppm. Usually ozone detectors are installed and proper interlocking mechanism is provided to ensure that public exposure is not exceeded beyond the permissible limits.

5.1 Identification of Initiating Events (IEs)
Some possible scenarios considered in this study, (centred on Indus facility) are: (1) excessive Bremsstrahlung in the ring due to loss of vacuum; (2) target failure due to excessively focused beam; (3) mis-directed / mis-steered beam; (4) beam loss and sky shine.

Exposure of personnel to direct Bremsstrahlung, neutron radiation (generated by the loss of high-energy electrons during operation of the accelerators and storage ring) and synchrotron radiation itself is prevented by permanent shielding and the Access Control Interlock System (ACIS) for the accelerator and beamline radiation enclosures. Thus, AICS plays an important role in preventing excessive radiation exposures.

5.2 Development of Event Trees for the IEs
For ensuring safety of personnel from exposure to radiation, elaborate Personal Protection system (PPS) and Radiation Monitoring system (RMS) have been devised and installed in Indus Accelerator Complex. The PPS consists of (i) search and secure, (ii) door interlocks, (iii) access control, (iv) CCTV and (v) public address facilities. RMS consists of a large ensemble of radiation monitors with alarms placed throughout the Complex. These systems cover the machine areas as well as the user beamlines. A typical event tree generated for mis-directed/mis-steered beam is shown in Fig. 1.

Consequence differs due to delay in closing of pneumatic valves (~2s) and needs to be analyzed.

<table>
<thead>
<tr>
<th>Frequency of Beam loss</th>
<th>Failure to trip the beam - FSS</th>
<th>Fail to trip safety valves</th>
<th>Consequence</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAFE</td>
<td>SAFE</td>
<td>?</td>
<td>UNSAFE</td>
<td></td>
</tr>
</tbody>
</table>

Fig. 1 — Event tree for beam loss scenario

Table 1 — Failure mode cause and effect analysis of initiating events

<table>
<thead>
<tr>
<th>Failure</th>
<th>Causes</th>
<th>Effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of vacuum</td>
<td>1. Improper flanges/gaskets</td>
<td>excessive Bremsstrahlung in the ring</td>
</tr>
<tr>
<td></td>
<td>2. Failure in pressure switches</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Power supply failure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Failure in cooling fans</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Breakage of Be window –</td>
<td>mechanical shock or oxidation</td>
</tr>
<tr>
<td>Target failure</td>
<td>due to excessively focused beam</td>
<td></td>
</tr>
<tr>
<td>beam loss</td>
<td>1. RF failure</td>
<td>mis-directed/</td>
</tr>
<tr>
<td></td>
<td>2. Shorted magnet</td>
<td>mis-steered</td>
</tr>
<tr>
<td></td>
<td>3. Optics failure</td>
<td>beam</td>
</tr>
</tbody>
</table>

5.3 System Analysis
System analysis looks into two aspects: estimating the frequency of initiating events and unavailability of mitigation system. Failure mode, effects analysis helps in understanding the failure modes of various components which results in system failure. It may be noted that only those failure modes that result in undesirable consequences are addressed in fault trees developed for the safety provisions/systems. Typical failure mode effects analysis conducted on some scenarios in accelerator are given in Table 1.

From the FMEA results, fault trees are drawn for the failure events (IEs) identified in FMEA table.
A typical fault tree for the initiating event-beam loss scenario (first header event tree shown in Fig. 1) is given in Fig. 2.

Consequences from these IEs can be reduced to a great extent by the safety system, access control interlock system. Various safety facilities/systems are provided to prevent undue radiation exposures in accelerators. These are described below:

5.3.1 Search and scram system

Sequence of actions is prescribed which involves searching area and confirming that inadvertent trapping of personnel has not happened before beam is switched ‘ON’. Also, scram facilities to initiate fast closing of safety shutter in beam lines are present, if such a situation is warranted. Since Search and Scram system relies heavily on human action, human reliability plays a significant role.

5.3.2 Radiation detectors

A monitoring system with built-in redundancy is provided to detect the radiation levels in the experimental areas outside the hutches. The purpose of this system is to switch off the beamline whenever higher radiation fields are detected outside the hutches. The monitor is integrated with the personnel access door interlocks to prevent room access when the radiation level in the room is more than that specified. The monitor generates visible and audible alarm signals if the radiation level exceeds preset limits. Periodic testing and calibration of detectors are essential in ensuring their proper functioning.

5.3.3 Access Control interlock system

Particular attention needs to be paid to the accessibility of the radiation areas (like storage ring, booster ring etc.) in accelerators. Personnel cannot have access to these areas while the beam is ‘ON’. Such control of access relies heavily on the use of interlocked systems. Sequentially interlocked controls are generally provided for personnel access and locking of the radiation areas. Opening the access door also switches off the high voltage supply for the beam. Redundancy is provided through, manual Corey lock system and through automated interlock systems. Any attempt to override the controls or apply them out of sequence must automatically abort the intended operation and require the sequence to be restarted.

Fault trees are also drawn for safety systems, e.g. failure to trip the beam (which is second header event tree shown in Fig. 1) as shown in Fig. 3.

Recent advancements in PLC based access interlock systems, introduces a new dimension and adherence to standards such as IEC 61511 to ensure high reliability of these interlock systems. IEC 61511 is performance based umbrella standard that applies to any industrial process that uses Electrical/Electronic/Process Equipment Safety related systems. It applies when functional safety is achieved using one or more safety instrumented functions (SIFs) in safety instrumented system (SIS) for the protection of personnel, public and environment.

In case of SIFs, probability of failure on demand (PFD) is characterized by Safety Integrity Level (SIL). SISs are composed of sensors, logic solvers, power supplies, field wiring, final control elements and communication interfaces and may include hardware, software and human intervention. Four
Discrete integrity levels (SIL 1 to 4) are defined as shown in Table 2. The higher the SIL level, the higher the availability of SIS. It is recommended that there are two channels of instrumentation each catering to SIL 2 for achieving SIL 3 for the access control interlock system.

These standards are based on safety life cycle concept, in which safety is defined, designed and maintained throughout the lifetime of the system. Design principles such as redundancy, defense in depth, diversity, test and maintenance of various equipments, etc. and proper verification and validation of the SIS at all stages are required to achieve the prescribed SIL level.

5.4 Evaluation of Risk

The outcome of PSA studies for these facilities is to generate a risk profile. A typical risk matrix is shown in Fig. 4. The risk matrix is depiction of the frequency of accident sequences and their associated consequences. It is desirable to have the plant risk towards the lower left corner of the risk matrix. In case it is in the upper right corner, changes need to be made in the design of the safety provisions/systems to bring it towards the lower left corner.

The probability values can be high (>10^{-1} per year), medium (10^{-2} to 10^{-1} per year), low (10^{-4} to 10^{-2} per year) or extremely low (10^{-6} to 10^{-4} per year). The consequences are categorized as high, medium, low and extremely low based on the impact of the incident (off-site and on-site). Typical scheme of risk indexing is shown in Fig. 4.

6 GAP Areas

PLC based system are increasingly being used in accelerator systems. Methods for assessing the reliability of these systems need to be explored and standardized. Periodic testing and calibration of radiation monitoring instruments is an essential pre-requisite to ensure that these systems meet the required SIL demand failure probability values. Bypassing ACIS is going to result in acute exposures to operating personnel and experimenters. Hence, methods to assure reliability of these interlock systems and the human reliability of the operating staff and experimenters in adhering to accepted, reviewed and approved safety procedures are absolutely essential to avoid undue radiation exposures.

7 Conclusions

Studies conducted for similar experimental facilities have identified that the radiation safety interlock system, used to control access to areas inside ring and the huches of beamline facilities have impact on the risks from these facilities. PSA methods that are followed in nuclear power plants and their advantages are presented. How such studies can be conducted for accelerator facilities is explored. This paper brings out advantages in employing quantitative aspects for identifying the scenarios, which can provide more reliable and safe operation of such facilities. The requirements for enhancing the reliability of the interlock systems are discussed in this paper. Finally, how risk can be presented in a risk matrix and its role in reduction of risk is highlighted.

There are many gaps still to be bridged for PSA techniques to be very effective in risk analysis of accelerator facilities. These are touched upon. Overall, applying PSA to these facilities will help in ensuring that safety is achieved and in ensuring high reliability of protection systems.

References


