Transactions of the 15th International Conference on
Structural Mechanics in Reactor Technology (SMiRT-15)
Seoul, Korea, August 15-20, 1999

Risk Management of Nuclear Power Plant Using Living PSA

Lekha Chowdhury

Bhabha Atomic Research Centre, India

ABSTRACT

In a Nuclear Power Plant (NPP) risk can arise from unidentified design weaknesses and insufficient or weak operational procedures. It is, therefore essential to know the baseline risk level and then to monitor risk implications of any Plant configurational changes due to test, maintenance and repair activities. Prior safety analysis using Probabilistic Safety Assessment (PSA), dependent essentially on design information, gives the baseline risk level. For safe and cost-effective management of NPPs, the PSA of the Plant should be continually updated so as to carry out plant operations keeping in view risk perspectives.

1.0 INTRODUCTION

Programmes like Living PSA (LPSA) are developed with a view to address the issue of risk both for configurational changes as well as operational actions in the NPP. Minimization of Risk in any plant requires an understanding and detailed evaluation of Risk both qualitatively and quantitatively. LPSA of an Indian Pressurised Heavy Water Reactor (PHWR) was developed to monitor risk in the plant at any time. This contains all the fault trees of important systems and event trees of important accident sequences required for the evaluation of various Risk measures.

2.0 PSA

PSA has been extensively used as a tool in the design evaluation process to identify weak links in the system and suggest modifications. Occurrence of an Initiating Event (IE) and failure of one or more safety systems leads to an accident sequence. PSA deals with the identification of dominating accident sequences relevant to the given design of a reactor system and relegating it to various systems and components including the operator. CDF is the top event evaluated as a measure of plant risk and is the summation of the frequency of various accident sequences. Safety system unavailability would depend on the logical combination of the failures of its associated components.

PSA uses fault tree analysis as a deductive tool. A fault tree relates component failures to a particular system failure through an event logic diagram. Logical operations like 'AND', 'OR',etc. are used to combine primary failures which

lead to the top event i.e. system failure. PSA of a plant contains information on the failure logic of various systems in the plant. It also contains the data relating to the equipment failure, their operation and maintenance. The failure logic of various systems in the plant are modelled using fault trees.

3.0 LIVING PSA

A software called Living PSA was developed. The software has a modular structure. Safety systems have modules for fault tree drawing and tree evaluation. In case of a process system the failure frequency of the system can be modified if required. There is a module containing event tree models. The fault tree models are stored and can be selectively displayed in an interactive manner. The fault tree incorporates design, test and maintenance data for various calculations. Each system tree is stored in the form of text and data files. Changes in the probability of failure of one or more components of a chosen system can be incorporated. The new fault tree is evaluated and displayed immediately. Effect of system unavailability on all accident sequences and Core Damage Frequency can be seen. Living PSA is a PC based user friendly software tool. The main menu of LPSA displays the various jobs that can be done by the software. Hot keys are used to go to various jobs. LPSA can be used to modify, update and reanalyze plant PSA so that it can be employed by the plant staff for guidance. It can also be used for training operators on system failure, events the system failure can lead to and the consequences of different possible plant states.

4.0 RISK MEASURES

Baseline CDF depends on the system design and their logical connections in the plant. This value is affected by the frequency of failure and downtime of equipments in case of operating systems (process systems) and by the the test frequency of equipments in case of safety systems.Various IE, Safety system failure, equipment failures, etc. can be ranked based on their total impact on plant risk. Quantitative risk measures are used for planning plant operations and maintenance.

Risk Achievement Worth (RAW) of a component is evaluated as the increase in plant Risk due to failure of the component. New CDF is evaluated with probability of failure of the component as 1.0. The ratio of new CDF to old CDF gives the RAW of the component. Similarly system RAW can be evaluated.

Risk Reduction Worth (RRW) of a component is evaluated as the decrease in plant Risk when a component is fully reliable. The new CDF is evaluated with the assumption that the component is fully reliable i.e. its probability of failure is zero.

To have a single measure for risk based ranking a combination of RAW and RRW is used. Birnbaum importance of a component is evaluated as the summation of RAW and RRW. Another measure is called Risk importance which is evaluated as the product of Birnbaum measure and the probability of failure of the component. For Risk based planning the importance of a component in a chosen system is evaluated. In the LPSA software the importance of a component in a system is defined as

$$= \frac{\text{Unavailability of a component in a system}}{\text{Unavailability of the system}}$$

Importance of various systems, depending on their contribution to plant risk, is assessed. The ranking of systems or components is required for system inspection planning.

5.0 RISK MINIMIZATION USING LIVING PSA

Some of the factors affecting plant risk, like design data, are fixed while others like Test Interval, Maintenance Downtime, etc. are variable and can be adjusted to minimize plant risk. LPSA software aims at adjusting these variable parameters to achieve the target risk. This information on change in system reliability or unavailability along with the change in CDF (risk involved) can be used by the operator to take safety based decisions :

i) When a component or system is not available, whether to continue power operation over the repair time of the fault or to shutdown the plant, that is the present CDF, which is higher than the design value, is acceptable or not?

ii) What should be the priority, with which the equipments are attended and put back into service, in case of several components being out of service? The component with a higher contribution to plant risk should be put back to service first.

LPSA also gives the operator the increase in frequencies of the affected accident sequences. Consequently he knows which safety systems should be in ready state. The LPSA program is illustrated alongwith an example. Figure 1 shows the fault tree of Emergency Power Supply system in a NPP. Use of PSA to evaluate the impact of different status of equipments is explained.

1. Evaluate RAW of a component. This factor decides the priority of restoring a component to service. A component with a higher RAW has to be maintained first. RAW of a DG is found to be 2.19. It means that the plant risk increases 2.19 times if any one DG fails in the plant. This can be ranked with RAW of other important equipments in the plant. Increase in risk due to multiple component failures, in the same system can also be evaluated.

2. Evaluate RRW of any component: In case of system or plant design modifications, a component with higher RRW should be given higher priority as this would result in maximum reduction in plant risk. RRW of DG is found to be 1.05. This means there is a 4% reduction in plant risk if a DG is fully reliable.

3. The change in plant risk due to change in test frequency of important components in safety systems can be used to decide if the test frequency should be changed based on available plant data. The test interval of a DG is assumed to be 48 hrs. If this were increased to 168 hrs, the increase in risk is 5.196.

4. During design stage the annual downtime of components is assumed to have a fixed value. For a operating plant this may be different. Effect of change in scheduled maintenance time on plant risk is evaluated. This helps to focus attention on components contributing more to plant risk due to their maintenance downtime. Scheduled downtime of EPS is 168 hrs. Observed plant data can be used to evaluate plant risk.

5. Actual test results, based on plant operating experience, can be used to find the unavailability of important components in safety systems and to ensure that the failure probability of components is maintainend as used in the design stage. All DGs

in EPS are tested once every 48 hours. If the test results show that there are 3 failures observed in 150 tests, this data can be

used to evaluate the actual failure probability of a DG. Now the DG failure probability is 2e-2. Optimum test interval now is evaluated as 72 hrs.

6. Changes in component failure probabilities can be used to study the result of possible combinations of failure of equipments in the plant. For example by using combined values from sections 3 to 5 as input to the system fault tree and entering the required values at component level the combined effect on plant risk found.

7. Changes in plant risk can evaluated based on actual operating experience of process system failure frequencies and safety system unavailabilities. For example, Power Supply failure frequency in design data is 1/yr. If the observed value is 2/yr then the plant risk is evaluated as 1.65. Similarly the change in plant risk due to more than one IE is evaluated.

CONCLUSION

Prior analysis should be carried out to evaluate the risk in any operating plant at the design stage. This gives a baseline data for ensuring that the plant maintains at least this level of safety. LPSA can also be used for drawing up System Inspection Plans depending on the risk importance of various components in safety systems. Risk based decisions can also be taken on test, maintenance scheduling, generating procurement procedures, supporting decisions on safety issues, identifying design and operational weaknesses and Training purposes.

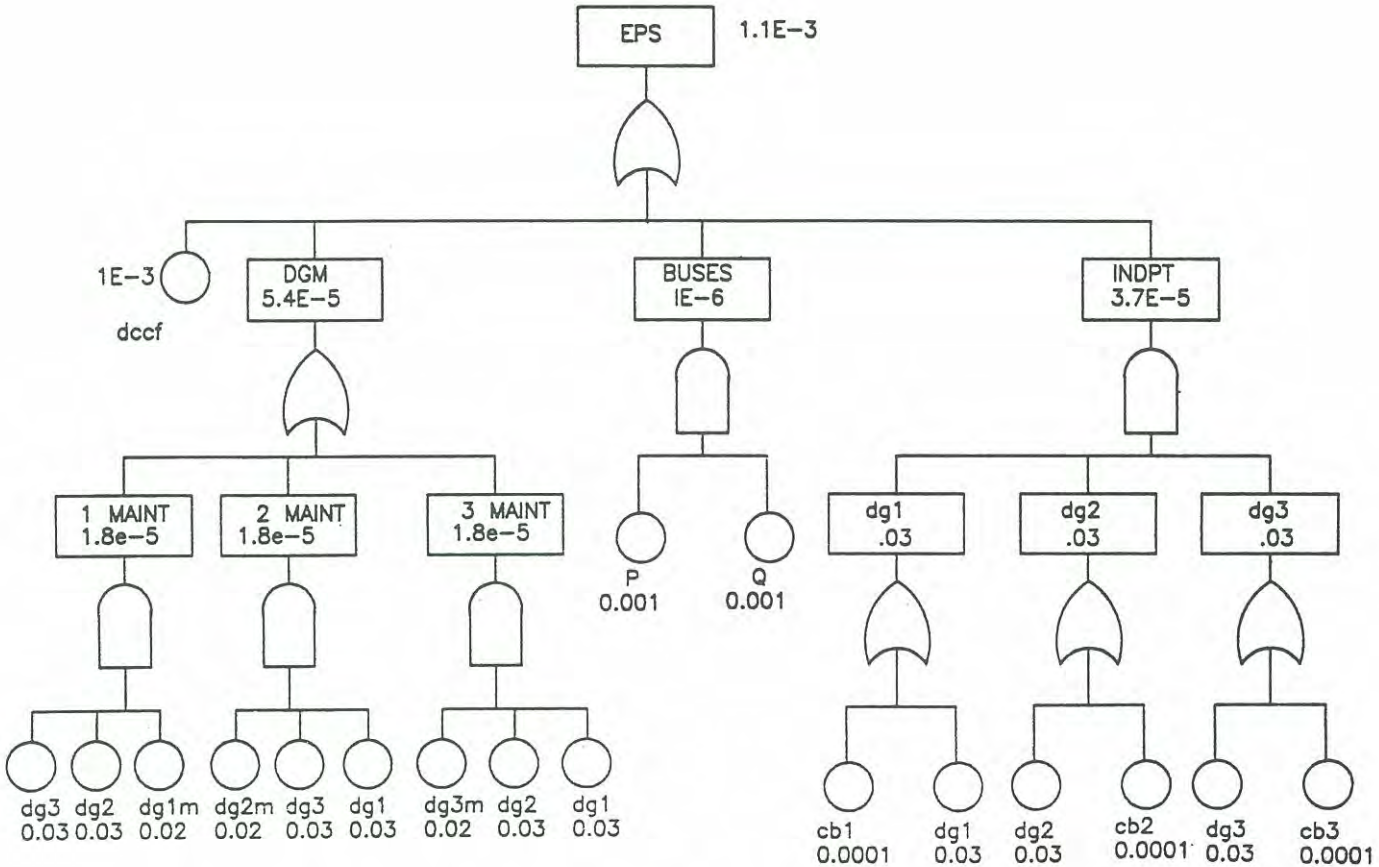

FIG.1: FAULT TREE : EMERGENCY POWER SUPPLY.