A Methodology for Living Probabilistic Safety Assessment (LPSA)

MUHAMMAD ZUBAIR1, ZHIJIAN ZHANG2
College of Nuclear Science and Technology
Harbin Engineering University
145-Nantong Street, Nangang District, Heilongjiang Province, city Harbin
CHINA
zubairheu@gmail.com

Abstract: - The objective of this paper is to summarize the latest techniques, applications, methodologies, use of different software, and development of codes, in the field of Living Probabilistic Safety Assessment (LPSA) and Risk Monitoring (RM). The paper consists of three parts, in first part definitions, history, aims, uses of LPSA, and a new detailed model for LPSA have been explain. In second part brief introduction, worldwide use of RM, benefits and draw backs of software in RM, and in final part comparison between LPSA and RM have been discussed. The study also makes recommendations for further use and development of these two techniques in present and future NPPs.

Key-Words: - Comparison, data base, LPSA methodologies, new model, risk monitoring, updating of LPSA,

1 Introduction
To make NPP more safe and reliable different techniques including defence in depth that prevents the release of radioactive material during the design process. This principle consists of five levels including prevention from normal failures, detection and interception of deviations, controlling the consequences of any accident, prevention from severe accidents, and safety from releases of radioactive materials [1]. Similarly in an organization the over all behaviour of individuals that effect organization’s health and safety programmes is known as safety culture [2], but with passage of time new concepts such as PSA come into action. According to the International Atomic Energy Agency (IAEA), PSA applications have been categorized in the following ways according to their purpose; safety assessment, design evaluation, NPP operation, permanent changes to the operating plant, oversight activities, and evaluation of safety issues. In order to use a PSA in the decision making process, it is necessary to define, important needed results and set a criteria to compare these results. In some cases, these results may be qualitative, but in most cases, these results are quantitative. In case of quantitative results, some parameters that can be calculated using the PSA model are defined, which are referred to as metrics. Typically used metrics are important measures for core damage frequency (CDF), large early release frequency (LERF), conditional core damage probability (CCDP), quantitative health objectives (QHO), etc [3]. Fault Tree (FT) and Event Tree (ET) play an important role in order to simplify PSA methodology. Failure of components or subsystems which can result in a failure of power delivery to specific loads or in certain cases in a full blackout of the power system can be solve by fault tree analysis and the power flow model [4]. Presently new systems of modeling approach for computer-aided fault tree generation are used. In these methods every system model is composed of some components and different types of flows propagating through them. Each component has a function table that describes its input–output relations. For the components having different operational states, there is also a state transition table. Each component can communicate with other components in the system only through its inputs and outputs. A trace-back algorithm is proposed that can be applied to the system model to generate the required fault trees [5].

There are few PSA methods for low power and shutdown (LPSD) period so by using reference FTs and applying conditioning methods to these reference FTs better results can be obtain. The conditioning method includes a condition gate function, an alternative FT structure and the substitutions of an event to a reference FT. In this method one can use the FT of a full power PSA as the starting point to maintain a consistency between
Maintaining the original structure of the FT for a full-power PSA and providing flexibility to develop FT for the LPSD was the key factors of this field of study. These methods have been applied at different power plants in Korea and results show that FTs for LPSD PSA model can be generated easily as compare to full power mode [6]. On the other hand the behavior of components of complex systems and their interactions such as sequence and functional dependent failures spares and dynamic redundancy management, and priority of failure events, cannot be adequately captured by traditional FTs. Dynamic fault tree (DFT) extend traditional FT by defining additional gates called dynamic gates to model these complex interactions. Markov models are used to solve dynamic gates. However, state space becomes too large for calculation with Markov models when the number of gate inputs increases.

To address these difficulties, Monte Carlo simulation-based approach is used these days [7]. Although these techniques are suitable for safety analysis but during operation of NPPs changes occur in components reliability and operating procedures which continuously modify configuration of NPP so in order to deal these situations LPSA and RM gives a new concept in maintaining and improving safety of NPPs. In this paper we try to review these two methods, comparison between them, and a new model for LPSA which will helpful to understand the idea of LPSA.

2 Living Probabilistic Safety Assessment (LPSA)

“Living PSA” (LPSA) can be defined as a PSA of the plant, which is updated as necessary to reflect the current design and operational features and is documented in such a way that each aspect of the model can be directly related to existing plant information, plant documentation or the analysts assumptions in the absence of such information. The LPSA would be used by designers, utility and regulatory personnel for a variety of purposes according to their needs, such as design verification, assessment of potential changes to the plant design or operation, design of training programmers and assessment of changes to the plant licensing basis. The core of LPSA is a risk model of the plant which adequately reflects the current design and operational features [8]. LPSA can also be defined in different ways such as a daily safety management system which is based on plant specific PSA and supporting information system. A dynamic PSA tool for accessing real plant configuration which is capable of producing results in useful time scale. LPSA is a technology which allows the performance of PSA within an appropriately small time period and which is up dated sufficiently regularly to remain valid at all times [9]. A system which uses PSA data and computer software to provide risk level and plant current working state is known as LPSA.

2.1 Methodology for LPSA

The basic method of LPSA is to calculate average risk and to support maintenance system. For this purpose detail knowledge for each component and each system of NPP is required; in order to achieve this goal different softwares are used as a tool of LPSA method. Risk assessment, risk monitoring, and risk follow up are three different approaches to use LPSA. The basic premise of a Stage 1 LPSA is that it is used as an off-line tool and its idea is related to basic PSA. Therefore this stage does not model the current state of operating plant i.e. changes in plant configuration and unavailability as they occur. The Stage 2 LPSA is an on-line time-independent LPSA and its purpose is to calculate instantaneous risk. In addition, it allows plant unavailability to be assessed as they occur at each point in time and may be used to plan maintenance outages in order to minimize risk. Stage 3 living PSA is an on line dynamic living PSA which is updated by plant operator when changes in plant configuration occur. It is dynamic in the sense that all standby components are modeled with respect to their last inspection time [10].

2.2 Proposed methodology

According to our proposed methodology LPSA model has two targets, first is the development of LPSA and second updating of LPSA. Our purpose for development phase is to calculate core damage frequency (CDF). On other hand updating phase gives us updating procedure, updating data base and applications guide lines. These are explain in fig.1.
2.3 Development of LPSA

The development of LPSA is consists of documentation, quality assurance, and organizations and resources. It is necessary that documentation is organized in such a way that it can be easily updated as changes occur. For this purpose task procedures and analysis of files are important. By keeping in mind these two techniques we can calculate internal initiating events evaluation, Event tree and success criteria analysis, System analysis using fault tree model, Common cause failure analysis, Human reliability analysis, Data analysis, FT and ET quantification to estimate CDF.

In this way we perform level -1 PSA and calculate CDF. In initial stage of our methodology we describe level 1 PSA because it will use in making LPSA application guide line. After the completion of level 1 PSA there are some uncertainties in the results, so Quality assurance (QA) is a tool to remove these doubts. The purpose of the QA plan and procedures are to ensure that the necessary documentation is developed and that the review process for all work products is clearly specified. QA program give us detail about how PSA work is to be manage, responsible organizations, objective and resources of PSA, internal and external communication, staff training, completion of documents, review of documents, verifications and validations of all codes and softwares used for PSA [11].

Organizations and resources include experienced and qualified staff, responsible departments, connection of departments so that any problem can be analyze and solve easily.

2.4 Updating of LPSA

The updating of LPSA involves documentation for updating, quality assurance and organization and resources, (as shown in fig. 1), but here we mainly focus on how to update LPSA. As during the calculation of CDF we have detail FT and ET, so if we change or reduced the size of FT or ET then we can easily update LPSA. For this purpose we have different methods like house event method, condition gate method, If Then Else logic method (ITE), change minimal cut sets, and development of modules.

In house event method the basic event depend on house event, if house event is true then basic event appear, but if house event is false then basic event will not appear. The condition gate and ITE method use to model complex situations. Condition gate method is not a conventional Boolean operator so it is difficult to check failure of basic event, however ITE is based on conventional Boolean algebra and hence it is better then condition gate method. So we can say that when conditioning part of FT is very big then condition gate method is better, but when conditioning part of FT is not complex then ITE approach is suitable [12]. Development of Modules can reduce the size of FT. In modulization the components that have same mutual logical relationship are combined so that we can easily find minimal cut sets [13].By choosing one or more methods we can change FT which means updating of LPSA. Reliability model parameters identification, component grouping, collecting generic information, plant specific data collection and evaluation, Derivation of plant specific parameters including CDF, handling of new equipments are important for LPSA updating.

2.5 LPSA update data base

The LPSA data base is a product of level 1 PSA, plant operational data and plant design data as mentioned in fig.2. Frequency of initiating events,
event trees, and fault trees are basic requirements of level-1 PSA. Component failure rate, repair time, maintenance frequency, test duration and list of LOCA (Loss of Coolant Accidents) are including in plant operational data. On other side all components list and diagrams are main parts of plant design data.

2.6 Application guidelines
To perform LPSA in systematic and consistent manner LPSA application guideline is a key factor. We proposed that with the help of Bayesian methodology the updated data can be used to Change plant design and operation and its results will helpful in making LPSA application guidelines as shown in fig.1. From fig. 1 it is also clear that updating data base and application guidelines have relation with each other, and their data information can be transfer during updating process.

3 Risk Monitoring (RM)
A 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 risk monitor reflects the current plant configuration in terms of the known status of the various systems and components, e.g., whether there are any components out of service for maintenance or tests. The risk monitor model is based on and is consistent with the LPSA. It is updated with the same frequency as the LPSA. The risk monitor is used by the plant staff in support of operational decisions [14]. The main purpose of risk monitor is to control the risk during plant normal operation and to calculate core damage frequency (CFD). Moreover, it can also be used to measure risk achievement worth, and risk reduction worth. The first risk monitor was developed by UK and put into operation in 1988, after this the number of risk monitors increase rapidly, and every country even every organization wants to make his own risk monitor. These days different software are used for risk monitoring including essential system safety monitor (ESSM), dynamic risk monitor (DRM), risk spectrum, risk man, fault tree analysis, equipment out of service (EOOS), paragon, and cosmos etc. A risk monitor called risk assessment tool (RAT) has been developed. Its key features includes development of graphical FTs and ETs, 30 days risk profile, handling time dependent failure data. This software has been applied to Tehran research reactor and noted that its results are better as compare to other software [15].

4 Comparison between LPSA and RM
When PSA analysts finish the analysis then problem appear that how to represent these results, but LPSA use techniques for safety assessment and risk management, made nuclear power plant system every day up to date [16]. A formally documented PSA model of a plant used to determine the average risk based on the expected unavailability of systems and components. It is updated on a regular, but not necessary frequent basis. Risk monitoring is a PSA model of the plant used to determine the instantaneous risk based on the actual status of the systems and components. It is updated on at least the same frequency as the LPSA for plant design and data but can reflect the current status of tests in progress and maintenance activities [17]. Since the observation period of PSA is very long so by using LPSA software such as risk spectrum different test strategies are possible with in limited time [18].

References:
[6] H. Gon Lim,J, Hee Park, S.Hoon Han, S.Cheol Jang, “Fault tree conditioning methods to trace


