# General design of on-line risk monitor for nuclear power plant

**ZHANG Zhijian [1], WANG He [1], and LI Songfa[1]**

*1.Fundamental Science on Nuclear Safety and Simulation Technology Laboratory, College of Nuclear Science and Technology, Harbin Engineering University, 145-1 Nantong Street, Nangang District, Heilongjiang, Harbin, 150001, P.R. China (wanghe@hrbeu.edu.cn)*

**Abstract:** On-line risk monitor (OLRM) used in nuclear power plants (NPP) is based on the fault tree/event tree models typically used in the probabilistic safety assessment of NPP. OLRM is different from the existing risk monitor for NPP in that it receives on-line risk information from I&C system through hardware. At the same time, this risk monitor can automate operation and update the on-line risk model and the reliability data of the equipment by receiving signals. So the OLRM is in the stage 4 of living PSA according to the Freeman's classification of the risk monitor. When the plant configuration changes, the risk monitor will get the results about instantaneous risk and component importance in time. This paper summarizes the features, structure and function of key parts of OLRM.

**Keyword:** on-line risk monitor(OLRM); probabilistic safety assessment (PSA); living PSA(LPSA)

## 1 Background

Nowadays the Probabilistic Safety Assessment （PSA） has rapidly become a well-established discipline with growing applications in support of decision making process in Nuclear Power Plant (NPP). It is primarily used to support the design and operation of NPP [1]. Currently, PSA models of many NPPs are maintained by Living Probabilistic Safety Assessment (LPSA) model. LPSA is a daily safety management system based on a plant-specific PSA and supporting information system [2].

LPSA has a quality that is suitable to support PSA applications for daily management of NPP. One specific and important application of LPSA is risk monitor (RM). LPSA model is the basis for the PSA model used in the RM. The main purpose to develop RM is risk-informed planning of operational activities, which includes test planning, maintenance planning and operational decision making which is based on the measurement of instantaneous risk [3].

In general, there are broadly three categories of LPSA which can be described with their advantages and application level [4]. They are as follows:

- *Stage1*: The LPSA is an off-line PSA which can be updated on a regular basis.
- *Stage2:* The LPSA is an on-line time-independent PSA, in which standby component failure probabilities are modeled at the end of their inspection period, and is updated by the plant operator when plant configuration (*i.e.* opening/closing section valves) changes or occurring plant unavailability.
- *Stage3*: The LPSA is an on-line dynamic PSA, in which all standby components are modeled with respect to their last inspection time, and is updated by operator when plant configuration changes or occurring plant unavailability, as well as when testing takes place.

The Stage 1 LPSA is used as an off-line tool to carry out assessments in advance of the systems being introduced/modified or in response to plant failure which have occurred. Therefore, it cannot model the current operating state with configuration changes in NPP [4].

The Stage 2 LPSA allows plant unavailability to be assessed when the configuration changes occur at each point in time. Therefore, it can be used to plan the allowed outage of plant in order to minimize risk [4]. An interactive LPSA for NPP has been developed to be used by operators and planners to give advice on the acceptability of plant unavailability from the viewpoint of the risk. It can be used to minimize and monitor the risk by maintenance activities. Also

**Received date: June 6, 2015**
(Revised date: June 8, 2015)

historical risk plots may be produced to give the time-averaged outage factor [4]. In practice, the plant unavailability states or changes in the plant configuration are required to be input by the operator manually and regularly.

The Stage3 LPSA is a natural extension of the Stage2 LPSA, and it removes conservative assumptions about 'end of test interval' [4]. Therefore, the Stage3 LPSA is required to be updated every time when a plant item is tested, or when the plant unavailability occurs due to maintenance and failure. By the application of Stage3 LPSA, it can monitor all standby system/ component by their test interval, and identify those items which will be significant to the planned outage by risk measure. Standby component failure probability will be reset to a lower value if the standby component is tested successfully in Stage3 LPSA, although it is assumed constant in both Stage1 and Stage2 LPSA. A Stage3 LPSA may provide more comprehensive advice to operator than other stages, and it can be used as a tool for developing a risk-centered maintenance strategy. However, many applications of Stage3 LPSA have not been implemented on a real-time basis [4].

Since the first RM which is called essential systems status monitor (ESSM) as the Stage2 LPSA was put into service at Heysham2 in 1988, there has been rapid growth of the number of risk monitors and nowadays more than one hundred are in service [3]. Moreover, a series of computer facility called dynamic risk monitor (DRM) as the Stage3 LPSA has been developed for NPP [4].

Although the configuration changes in NPP and updating of risk model were considered in the currently used RMs, they still ignore the stochastic events and automatic continuous operation activities which are closely related to risk. Moreover, real-time and automatic basis RMs are not yet established and the deficiency in acquiring quick and accurate risk information. In summary, the conventional RM is inadequate for on-line incident management.

## 2 OLRMS and its features

With the development of digital I&C systems and computer technology in NPP, more information can be accessed in short time. Meanwhile, the technological breakthrough of the RM was the calculation speed by which it is able to solve the plant PSA model. While complete solution of the plant model to calculate the core damage frequency (CDF) required hours and even days in the past, the current version of the RM accomplishes the CDF calculation which includes the LERF evaluation roughly in one minute on a Pentium PC [5].

Therefore, the RM developed with capability of fast calculation and automatic updating can model time-dependent state of the NPP, and it can perform the real-time calculations. In order to achieve such an application of RM, the stage4 LPSA will be newly required, the feature of which is described as follows:

- *Stage4:* The LPSA is an on-line time-dependent PSA which combines the on-line NPP state monitoring technique and the predicting technique, in which risk model is developed as on-line in time automatic update by signals, on-line time dependent (mission time, updating failure probability) and on-line data analysis and restore.

Based on the above-stated idea of stage4 LPSA, the on-line risk monitor (OLRM) system has been under development by the authors of this paper, in order to support the decision-making process of operators and managers in NPP. At present, the basic design of OLRM considers the conditions of full power operation with considering internal events and level 1 PSA.

The OLRM under development reflects the current plant configuration on-line at any given time. The OLRM can carry out on-line incident management such as risk assessment of current stochastic events and current planning failure activities. As well as optimization of experiments and testing activities in NPP can be achieved off-line. The calculation of all risk related operational activities is required to be accurate and timely.

To sum up, there are some important features of the authors' developing OLRM. They are (i) online operation, (ii)access to risk information in time, and (iii) risk assessment in the short term, as will be discussed individually.

### 2.1 On-line operation

In order to ensure the on-line operation of system, the OLRM is developed as on-line linkage to I&C system and other information system.

Through analyzing the monitored signals and planning the activities in time, the OLRM can get the plant configuration information continuously so that the on-line risk model and the reliability data of the equipment can be updated automatically in time. Also, the instantaneous risk and other risk information will be calculated immediately, which can support the users to make decision. The hardware structure design of OLRM is shown as Fig.1.

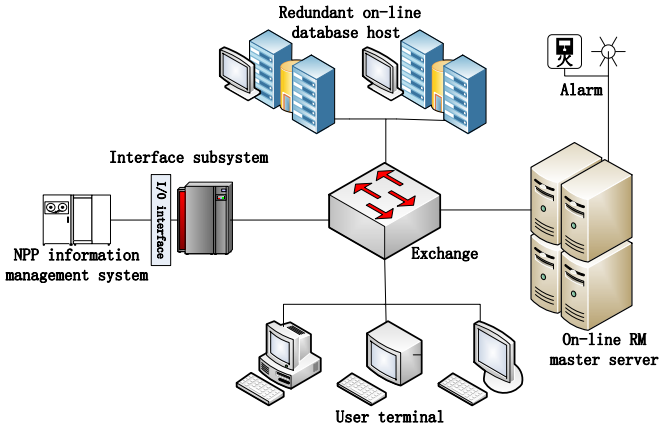


Fig.1. Hardware structure design of on-line operation.

### 2.2 Access to risk information in time

In order to timely access the various types of risk information, OLRM is required to calculate the risk immediately and get results in two minutes when changes or unavailability in NPP is occurred. For example, the Allowed Configuration Time (ACT) can be got in two minutes after every change. Moreover, OLRMS is also required to calculate the risk which varies with time even no change occurs in NPP. OLRM normally calculate risk model once at every updating time. However, it may calculate many times for routine maintenance activities, especially for large maintenance activities.

### 2.3 Risk assessment in the short term

The OLRM perform the on-line basis risk assessment, so that it mainly carry out on-line short term applications such as *status monitoring*, *current planning activities* and *Incident management*. The incident management is a typical OLRM application and deals with severe situations at the plant where rapid decisions are needed[3]. To sum up, the OLRM evaluates the instantaneous risk to provide support for operational risk decision making in the short term.

The severity is controlled by on-line monitoring. The maintenance actions can be prioritized so that the most critical systems are repaired or maintained first, or some specific maintenance isolation are postponed. Success path importance such as risk decrease factors can be used to rank the actions. A test importance type of measure can be used to decide whether some action is worth performing [3].

Therefore, OLRM has a short-term and an on-line in time evaluation perspective. The results from OLRM produce quantitative and qualitative risk measures. These will include the instantaneous Core Damage Frequency (CDF), minimal cut sets and the order of importance degrees, and numerical values which include baseline risk, annual average risk, continuous instantaneous risk, annual cumulative risk, and incremental risk [2]. The following characteristics need to be controlled:

- Real-time operational status. (Running, standby, isolated, open, closed, in maintenance, repair or test, *etc*.)
- System and component availability. (Systems and components are out of service or being restored)
- Changes of system/component configurations. (Change of operational train and stand-by train, opening/closing valves, *etc*.)
- Maintenance schedule.
- When periodic tests are performed.
- Component reliability parameters are updated automatically. (Updated by running time, repair times, demand times, test intervals, maintenance intervals, failure rates, and per demand failure probabilities)

- Initiating event frequencies are updated in time. (By the way of updating automatically and manually)
- OLRM PSA model is updated automatically. (For example, if one or more operational or stand-by device break down, the rank of common cause failure (CCF) model need to be reduced)
- Environmental factor. (Changes in the environment causing increased failure rate/ probability, such as a higher probability of loss of off-site power in case of storm)
- Complete and continuous risk curve. (Indication of current risk level at a given time in the form of a number, historical risk level is shown as continuous curve, and predicted risk level is calculated by recent maintenance schedule or periodic tests)

## 3 Structures of OLRM

In the structures design of OLRM, the first consideration is about the physical relationship between OLRM and the external entities, as well as the information of data flow. The level 0 data flow diagram of OLRM is as shown in Fig.2.

On the basis of level 0 data flow diagram of OLRM, various internal subsystems of OLRM can be designed to deal with both the external input information and the internal calculation information. The level 1 data flow diagram of OLRMS is as shown in Fig.3. It describes the relationship between OLRM and the external interfaces. It also presents the data flow process of various internal subsystems in detail.

The OLRM is normally connected with the operator support system (OSS), digital control system (DCS) and risk-informed management system for operation and maintenance of NPP. They are all part of the information management system (IMS). At first, OLRM will get the operating data of NPP from the record unit and the condition monitoring unit of OSS, and then update LPSA model and reliability parameters of equipment by judging the configuration state of NPP in order to calculate the risk model immediately. Then, based on the calculated risk information, OLRM will provide an alarm signal to the DCS, or will provide the operating advice to the risk-informed management system for operation and maintenance management activities. Finally, NPP operators and managers can receive risk information timely from risk-informed management system in order to support their proper decision making.

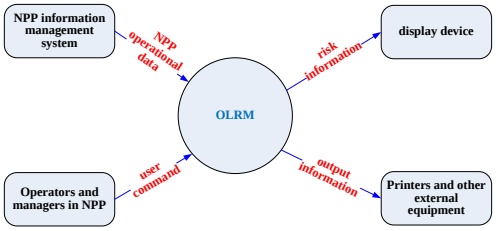


Fig.2. Level 0 data flow diagram of OLRMS.

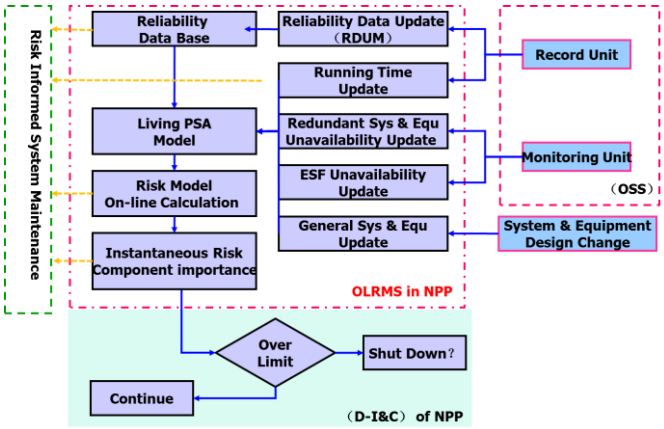


Fig.3. Level 1 data flow diagram of OLRMS.

The working of OLRM can be described in detail by presenting software structure design of OLRM operation, which is as shown in Fig.4.

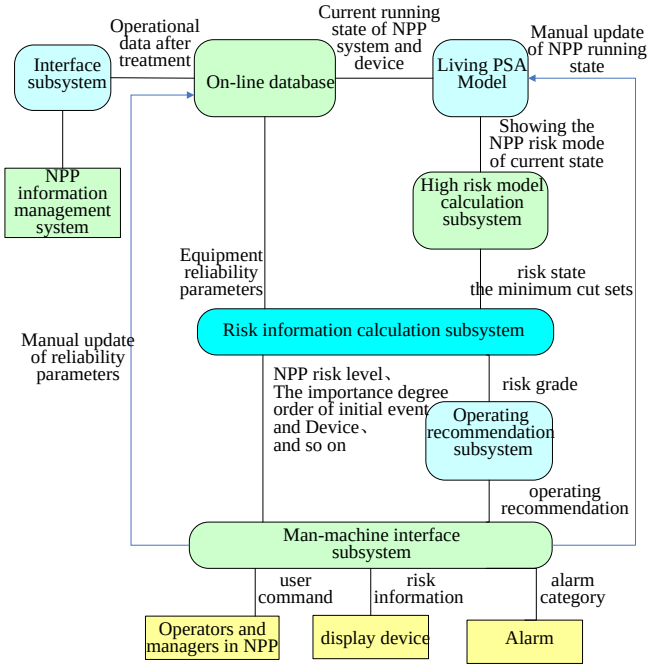


Fig.4. Software structure design of OLRM operation.

In the software structure of OLRM, the interface subsystem (IS) will get real-time operational data from IMS of NPP and then will convert the received data to the data type which OLRMS can identify to be input to on-line database. On-line database stores the status of events (basic event, middle event or top event) in risk model, the information about scheduled status changes (*i.e.* change of operational train and stand-by train, opening/closing valves), the information about time (running time, mission time, scheduled maintenance/test time, test intervals, maintenance intervals), the information about the recorded times (repair times and demand times), failure rates, and per demand failure probabilities, as well as other information about current plant configuration changes.

Based on those information, the equipment reliability parameters can be automatically updated. On the one hand, the cumulative failure probability of devices $F$ can be calculated by the equipment running time. On the other hand, the equipment failure rate $\lambda$ and failure-on-demand probability $P$ can be estimated by the basic event parameters and operational data. This also can achieve the function of long-term reliability data accumulation in NPP.

According to the current running status of the systems and equipment of NPP, OLRM PSA model can update risk model's basic events, middle events and top events, where possible, as well as the logical structure of risk model. On the basis of current updated risk model, the high risk model calculation subsystem can solve the minimal cut set equation of current state, such as CDF minimal cut set equation or LERF minimal cut set equation. Combining the reliability parameters from on-line database and the minimal cut set equation, the risk information calculation subsystem can provide various risk level, various order of importance degrees (such as the order of importance degrees of initiating event, the order of importance degrees of devices) and ACT as output. Finally, all of the risk information can be displayed reasonably by man-machine interface subsystem.

# 4 Function of key parts of OLRM

In order to achieve the goal of above design, OLRM will include the following five key parts as mentioned below with their functions:

- *Part1*: Reliability Data On-Line Acquisition, Analysis and Storage System.
- *Part2*: On-Line Risk Model Update.
- *Part3*: On-Line Risk Model Calculation.
- *Part4*: Operation recommendations.
- *Part5*: Human-Machine Interface.

## 4.1 Part 1: Reliability data on-line acquisition, analysis and storage system.

Reliability data on-line acquisition, analysis and storage system provides reliability parameters for OLRM, and the data in the system is stored in an on-line database. Therefore, the model data can be collected automatically from the plant monitoring systems. Meanwhile, the reliability data accumulation is in the life cycle of nuclear power plant. Also the purpose of this part 1 is to link the risk monitor to other information systems in the plant, such as digital control system (DCS), fault diagnosis system (FDS) and test and maintenance scheduling software.

## 4.2 Part 2:On-Line Risk Model Update.

The purpose of this part 2 is to update risk model when the plant configuration will change. The OLRM should include functions that update model automatically to

demonstrate the status and reliability parameter of the plant. This can be achieved by the following ways:

- Include functions in the risk monitor that allow modeling the current status of the plant by changing the logic structure in the model.
- Add the dynamic updated parameters model to the OLRM PSA model of the plant.

The updated level of structure includes basic event and middle event. The updating parameters include running time, mission time, scheduled maintenance/test time, test intervals, maintenance intervals, repair times, demand times, failure rates, per demand failure probabilities, environmental factor, rank of CCF and so on.

### 4.3 Part 3:On-Line Risk Model Calculation

The On-Line Risk Model Calculation (ORMC) is used to generate both the qualitative and quantitative analysis results of on-line risk model with model structure and reliability data updated in 2 minutes. The function of On-Line Risk Model Calculation is shown as Fig.5.

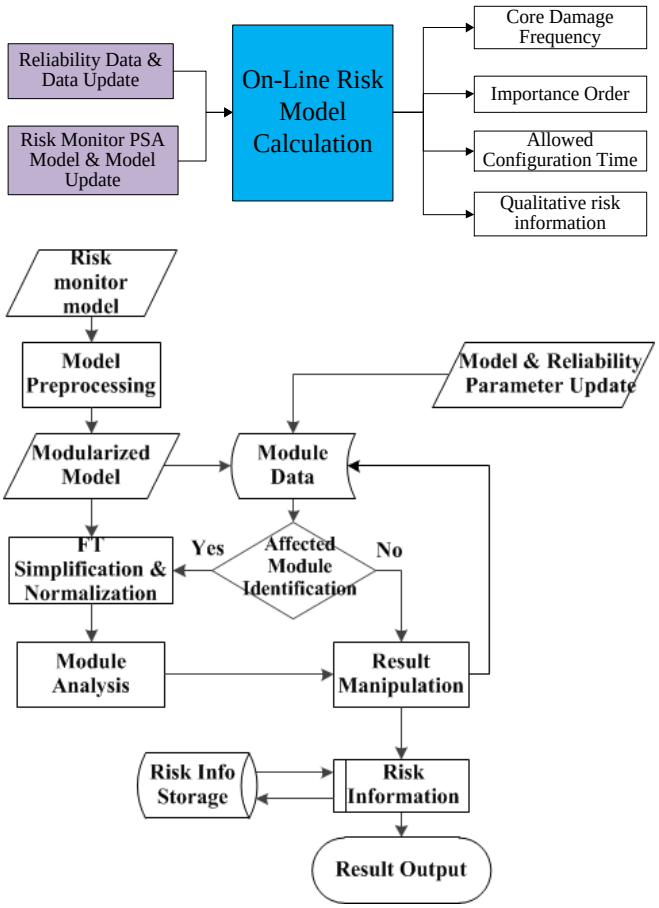


Fig.5. Function of on-line risk model calculation.

The OLRM should also be able to deal with operational procedures, test/maintenance schedules and other model status required in an off-line way. Therefore it may calculate many times.

### 4.4 Part 4: Operation recommendations

The operational recommendations focus primarily on the identification of hidden weaknesses when the plant configuration will change or provide an idea to support operators to reduce the risk level of plant.

The operational recommendations are based the information as given below:

- Core damage frequency (CDF).
- Allowed configuration time (ACT).
- Component importance.
- Restoration advice.
- Important Component sensitivity analysis.

### 4.5 Part 5: Human-Machine Interface

Human-Machine Interface should be designed as user friendly interface. When designing risk monitor software, the user must be defined so as to meet the actual operation requirements of the plant. The most important requirement of OLRM to be designed will be for the users who are not proficient in PSA technology.

Human-Machine Interface should be general. The interface is not in itself specific for each plant, but the interface is adaptable to each plant's specific requirements with regards to the defining plant configuration, defense-in-depth, and so on.

Human-Machine Interface should mainly include the following two functions:

- Change the configuration manually and automatically.
- Demonstrate the risk information calculated reasonably.

## 5 Conclusions

It can be seen from the foregoing discussion that some requirements for OLRM are very important, such as operating in real-time, by following the plant current configuration, by calculating and analyzing model in a timely manner and the most important

issue will be that it can be used by plant staff with no knowledge of PSA techniques.

The OLRM concept proposed in this paper is different from the existing RM software. Concretely, it is in stage 4 of LPSA and it combines the on-line state monitoring technique with the predicting technique of NPP. In the proposed OLRM, the risk model should be developed as on-line in time automatic update by signal, on-line time dependent and on-line data analysis and restore.

The incident management is the typical application of the proposed OLRM, which is the most different feature from the conventional RM. Besides that, the OLRM can provide an off-line application of risk optimization process of testing and maintenance activities.

At present, some challenges still exist in development of OLRM. Firstly, the user's acceptance and the suitability of the software for actual operational requirements must be taken into account in NPP. This is very important issue. Secondly, the validation and verification of the proposed OLRM concept should be carefully considered. Finally, the development of on-line risk model calculation software will need continuous improvement which will mainly include the speed and accuracy of calculation as well as the functional stability.

## Acknowledgment

This paper is funded by the international Exchange Program of Harbin Engineering University for Innovation-oriented Talents Cultivation. And the project has been supported by the Nuclear Power Plant Living-PSA and Online Risk Monitor and Management Technology Research program financed by the National Science and Technology Major Project of China (project number 2014ZX06004-003) and the Nuclear Power Plant Online Risk Monitor and Management Technology Research program financed by National High-tech R&D Program (project number 863 Program) (2012AA050904).

## References

[1] KAFKA P.: *Living PSA-risk monitoring—current use and developments*, Nuclear Engineering & Design, 1997, 175 (3):197-204.

[2] CSNI: *Risk Monitors-The State of the Art in Their Development and Use at Nuclear Power Plants*, France: OECD NEA, 2004: 45-46, 77, v, 123-124

[3] SKI Report 94:2, *Safety Evaluation by Living Probabilistic Safety Assessment. Procedures and Applications of Operational Activities and Analysis of Operating Experience*, *Gunnar Johanson*, Jan Holmberg, January 1994.

[4] FREEMAN02R. I., and MOIR02G. R.: *What is living PSA?*, Nuclear Energy, 1993.

[5] SHAN H. C., HOOK T. G., and LEE R. J.: *Use of the Safety Monitor in operational decision-making at a nuclear generating facility*, Reliability Engineering & System Safety, 1998, 62:11–16.