Use of Probabilistic Safety Assessment for Configuration Risk Management in a Nuclear Power Plant

Jiaqing Chen[a*], Xuhong He[b], Yong Cao[a], Yi Zou[c], Johan Sörman[b]
[a] CNNP Nuclear Power Operations Management Co., Ltd, Haiyan, China
[b] RiskSpectrum AB, Solna, Sweden
[c] RiskSpectrum AB, Beijing, China

Abstract: Risk-informed probabilistic safety assessment (PSA) applications have been successfully implemented in some nuclear power plants worldwide. This paper introduces the utilization of PSA in configuration risk management (CRM) within a nuclear power plant employing risk monitor software. The risk monitor software interfaces with various plant information sources to access real-time plant statuses, triggering calculations of plant risk levels (e.g., Core Damage Frequency (CDF) and Large Early Release Frequency (LERF)) using the living PSA model. After calculation, the tool provides crucial PSA insights such as the Allowed Configuration Time (ACT) and equipment importance measures. The paper also outlines domestic regulatory requirements pertinent to CRM in China and delineates the implementation of the risk monitor to meet these requirements and enhance plant safety and operational flexibility. Finally, the paper highlights the need for further research and development in CRM related to both PSA models and software tools.

Keywords: Configuration risk management, PSA application, Risk monitor

1. INTRODUCTION

Risk-informed probabilistic safety assessment (PSA) applications have been successfully implemented in some nuclear power plants worldwide. One of the important PSA applications is configuration risk management (CRM). CRM is an integral part of nuclear plant processes and is essential to effectively assess and manage the increase in risk that may result from proposed maintenance activities.

In China, National Nuclear Safety Administration (NNSA) published the technical policy "Application of PSA in nuclear safety" for guidance of PSA applications in February 2010 and initiated several PSA application pilot projects in August 2012. In 2017 NNSA issued the “Technical Policy for Improving the Effectiveness of Nuclear Power Plant Maintenance (Trial)”, guiding nuclear industry to monitor and manage the effectiveness of maintenance of structures, systems and components (SSCs) and the risks of maintenance activities [1]. In 2019, NNSA issued the “Technical Policy for Configuration Risk Management of Nuclear Power Plants (Trial)”, requiring nuclear industry to conduct CRM for nuclear power plant operation and maintenance activities in accordance with the technical policy, establish and optimize the nuclear power plant CRM system, so as to improve the scientific and effectiveness of nuclear safety management decisions [2].

Currently CRM has been implemented in many operating nuclear power plants in China. CRM peer review is ongoing with regard to PSA model, CRM software functionality as well as CRM management systems.

This paper introduces the utilization of PSA in CRM within an operating nuclear power plant employing risk monitor software. The risk monitor software interfaces with various plant information sources to access real-time plant statuses, triggering calculations of plant risk levels (e.g., Core Damage Frequency (CDF) and Large Early Release Frequency (LERF)) using the living PSA model. After calculation, the tool provides crucial PSA insights such as the Allowed Configuration Time (ACT) and equipment importance measures. The paper also outlines domestic regulatory requirements pertinent to CRM in China and delineates the implementation of the risk monitor to meet these requirements and enhance plant safety and operational flexibility. Finally, the paper highlights the need for further research and development in CRM related to both PSA models and software tools.

2. CRM Regulatory Requirement in China

CRM is a method that uses the live probabilistic safety analysis model to calculate risk indicators according to the actual operation configuration of nuclear power plants, and carries out risk management of nuclear power plants. The risk indicators commonly used in nuclear power plants are level 1 CDF and level 2 LERF.

The implementation process of CRM includes three steps:

- determining the risk thresholds,
- establishing the risk management matrix,
- evaluating the configuration risk and taking corresponding risk management measures.
    - In case of equipment unavailability in operation, CRM risk assessment shall be performed within 1h, and risk managing measures shall be taken according to assessment results
    - Allowed Coregulation Time (ACT) shall be calculated and counted once CRM risk is in yellow zone
    - ACT is calculated based on ICDP<1E-6 and ILERP<1E-7 (final ACT is the smaller value calculated from ICDP criteria or ILERP criteria)
    - After risk evaluation and implementation of risk managements measures, the ACT could be extended to 10 times

The proposed instantaneous risk thresholds (for online risk management) are in Table 1.
The proposed cumulative risk thresholds (for maintenance risk management) are in Table 2.
The general risk management matrix is in Table 3.

Table 1. Instantaneous risk thresholds

Risk Zone	**CDF**	**LERF**
Unacceptable risk zone (Red)	≥1E-3	/
Risk management zone (Yellow)	≥200% baseline CDF	≥200% baseline LERF
Normal control zone (Green)	＜200% baseline CDF	＜200% baseline LERF

Table 2. Cumulative risk thresholds

Risk Zone	**ICDP**	**ILERP**
Unacceptable risk zone (Red)	≥1E-5	≥1E-6
Risk management zone (Yellow)	≥1E-6	≥1E-7
Normal control zone (Green)	<1E-6	<1E-7

Table 3. Risk management matrix

Operation (Random unavailability)	**Risk zone**	**Maintenance (Planned unavailability)**
Acceptable risk, normal maintenance arrangement	Normal control zone (Green)	Normal work control
Risk needs to be controlled, maintenance shall be finished as soon as possible, and compensation measures could be adopted in the meantime	Risk management zone (Yellow)	Assess non-quantifiable factors, and implement risk management measures
Unacceptable risk, measures shall be taken immediately	Unacceptable risk zone (Red)	One shall not intentionally enter this configuration

3. Risk Monitor software

3.1. General Features

The risk monitor tool being used is the Web-based RiskSpectrum® RiskWatcher (RWWeb) developed by RiskSpectrum AB [3, 5].

The RWWeb is designed to be used by both PSA knowledgeable and non-PSA knowledgeable personnel. Most of the Risk Monitor users are assumed to not be familiar with PSA model. The application therefore uses the normal plant equipment IDs and descriptions and a minimum level of PSA related terms.

RWWeb enables plant operators and schedulers to evaluate the plant risks associated with scheduling and approving online and outage maintenance activities, and will help plant personnel better understand the risks in any plant configuration.

The RWWeb supports the following primary functions:

- Logging historical records of actual plant configurations
- Online activities risk evaluation
- Maintenance planning risk evaluation
- Providing quantitative CDF, LERF, and respective accumulative risk
- Providing qualitative defence-in-depth analysis
- Providing information on the risk importance of the components that are in service as well as out of service

One of the key features in the RiskWatcher is that all model related data is edited in the baseline PSA model and no changes need to be introduced "afterwards" in the separate risk monitor model. The event information about changes in plant configuration is stored in RiskWatcher, and thus separately from the PSA model data. This principle simplifies the process of going from a living PSA baseline model to a functional risk monitor model and will greatly simplify continuous update work - i.e. maintaining a true living PSA model.

The RWWeb supports the blended approach of risk-informed decision making by providing qualitative and quantitative evaluations. The instantaneous risk can be quantified according to the changes of plant configuration. Example important risk information can be presented in RWWeb:

- A risk profile showing the risk level over time
- Comparison of different risk curves for different plans
- Cumulative risk for a duration
- Indication of current risk level at a given time point in the form of a number (relative or absolute risk), and in the form of colour indication e.g. green, yellow, orange and red
- Qualitative "defence-in-depth" status, which shows whether safety functions, systems, sub-systems and components are available, minorly or significantly degraded or unavailable e.g. green, yellow, orange and red
- Importance measures showing how important components, systems are in terms of contributing to current risk, or in terms of possible reduction of current risk

3.2. Web-based Application

The RWWeb is a web-based application. In comparison with traditional desktop-based applications, the web application has some distinct advantages:

- Easy to deploy
- Easy to maintain and update
- More accessible
- More traceable
- Platform independent, better adaptability and compatibility

The web applications avoid the burden in deploying on each client machine. No installation is required for the users, since all the deployment and maintenance work will be concentrated on the server side, and the users only need the standard web browser to access to the application. These characteristics have made it ideal for the Risk Monitor application. The web-based Risk Monitor is easier to use, and has the possibility to be more widely used, which is of great significance for the promotion of Risk Monitor application, and thereby be very helpful to the plant safety management.

The RWWeb is a natural multi-user application, and it is easy to provide collaboration between multiple users, as all data are centralized. Multiple users are able to access the same model data and plant configuration information at the same time. Multiple users can simultaneously perform many standard functions on the same model dataset without affecting other users or their data. These standard functions include but are not limited to, viewing risk profile, tracing operation log, performing individual What-if analysis, printing reports, etc. In

the RWWeb, logic check has been introduced before editing operation event log to prevent timing errors due to event log edited by more than one user at the same time.

Calculation speed is one of the key issues for a real-time Risk Monitor application system. It becomes even more important for a web-based Risk Monitor since there might be many concurrent calculation requests. In the RWWeb, a series of measures have been taken to improve the performance of quantifications. Quantification based on fault tree logic from PSA model solved for each new plant configuration is applied for RWWeb due to requirements of accuracy.

3.3. Automatic Import of Operational Log and Maintenance Plans

RiskWatcher Connector (RWC) is a tool that is designed to read event log data from a desired data source, convert, and merge it with logs in RiskWatcher database.

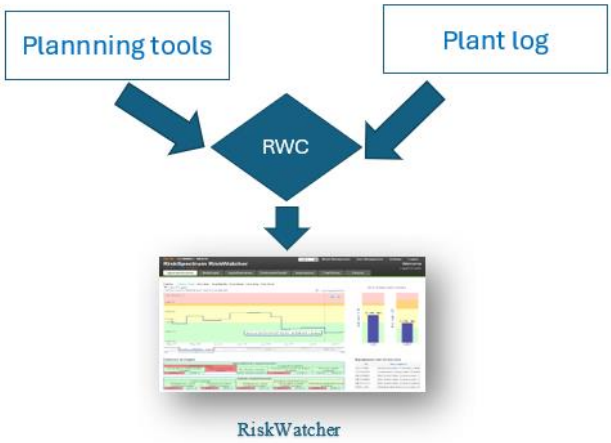

Figure 1. RiskWatcher Connector

RWWeb has good interfaces with the plant's existing information system. RWC will read relevant status signals of equipment from plant information system, convert to equipment status based on mapping rules and update in RWWeb upon the changes of status/configuration. Calculation will be automatically initiated after configuration change and the risk profile will be refreshed after completed calculation.

In theory no operator intervention is required during the whole process of operation risk updating by using this function. It can reduce the workload of using risk monitor for operational risk monitoring, and increase the accuracy and real-time characteristics of risk monitor. Feedback from the power plants indicate that there is almost no time delay caused by automatic input of plant configuration change. The major time delay for online operational risk monitoring is the PSA calculation time. For quality assurance of the automatic updating of the plant configurations, the users should review all the imported logs.

3.4. CRM features

Operational CRM is activated in the event of an abnormal event resulting in the unavailability of one or more safety-critical equipment. RWWeb is used to evaluate instantaneous CDF and LERF. Depending on the risk zone, corresponding actions will be taken, in addition to requirements specified in the technical specifications. When in the yellow zone, the maintenance/repair action needs to be completed as soon as possible: (1) the ACT is determined by the calculation of the cumulative risk ICDP and ILERP, (2) and compensatory measures need to be taken if necessary; In the red zone, immediate action is required to reduce the risk, and if the unit is in a power operation state, immediate shutdown and withdrawal are required to bring the unit to an acceptable level of risk.

Figure 2. Operator Screen for Operational CRM with ACT values

For maintenance CRM, it is consistent with the requirements of the maintenance rule. Before the implementation of maintenance activities, RWWeb is used to evaluate the configuration risk of the maintenance plan, and corresponding actions are to be taken according to the risk area. When risk is in the yellow zone, it is necessary to evaluate non-quantifiable factors and develop risk management measures; If risk is in the red zone, it is not allowed to enter the risk configuration. If the evaluation results indicate that there is a high risk of carrying out the planned maintenance activities under the current configuration, it is needed to adjust the maintenance activity time window.

4. Ongoing and further developments

With the implementation of CRM in the multiple NPPs and peer review findings, further research and development needs will be defined and implemented. This mainly includes:

- PSA model scope and quality: PSA model is continuously being updated. The model peer review findings will be addressed appropriately.
- Risk Monitor software user interfaces: two dashboard pages are being developed to combine relevant risk insights. One dashboard page is for operator online risk management and one dashboard page for maintenance planning. ACT information is to be presented together with other risk insights such importance measures, risk curves and accumulative risk values for the selected current configuration/timepoint.

- RWC integration into RWWeb: to provide a convenient way to add/import logs to a plan via RWC on RWWeb page instead of opening RWC application separately. Custom data source for RWC is supported.

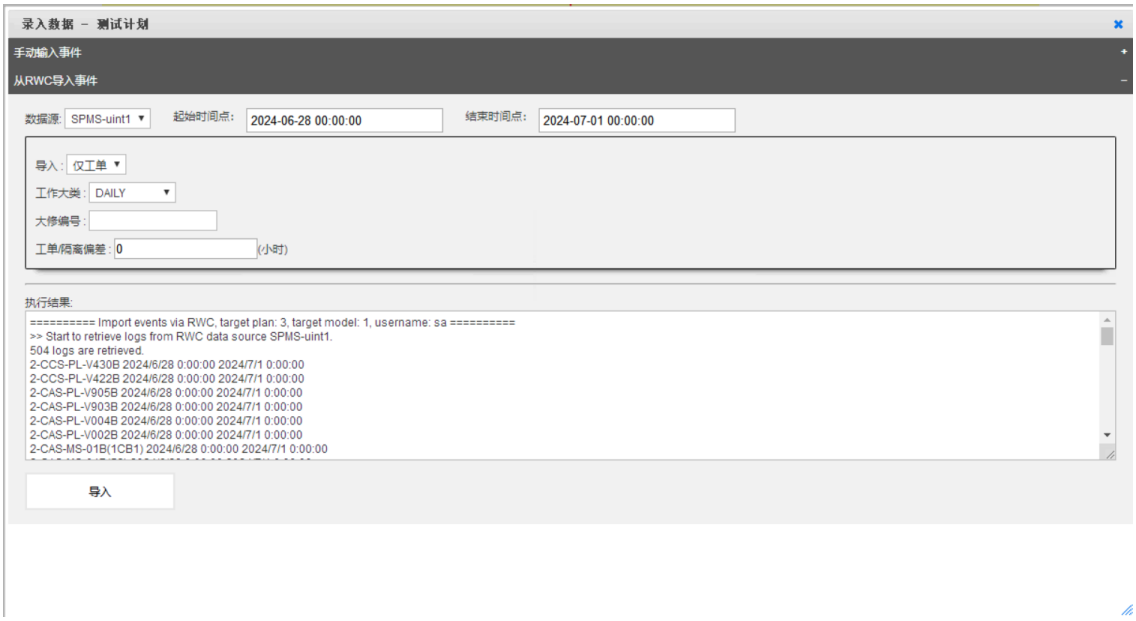

Figure 3. RWC integration

5. CONCLUSION

With the Configuration Risk Management (CRM) application, Risk Monitor will play a key role in NPP operation management, and one can expect to obtain actual benefit in operation flexibility.

The RWWeb fulfills the essential requirements for risk monitor. The web-based framework brings lots of inherent advantages including the flexibility to deploy and manage the application, better adaptability and compatibility, more accessible, etc. Automatic operation log import significantly reduces the workload of operator in using risk monitor and increases the precision of configuration input. Risk Monitor becomes highly integrated with plant systems and plant operating processes.

References

[1] China National Nuclear Safety Administration. Technical Policy for Improving the Effectiveness of Nuclear Power Plant Maintenance (Trial), 2017.
[2] China National Nuclear Safety Administration, No. 262. Technical Policy for Configuration Risk Management of Nuclear Power Plants (Trial), 2019.
[3] RiskSpectrum AB. RiskSpectrum® RiskWatcher Web User Manual, 2023
[4] OECD NEA, "Risk Monitors: State of the Art in their Development and Use at Nuclear Power Plant", NEA/CSNI/R(2004)20, 2004
[5] Hao Zheng, et al. Application of Web-based Risk Monitor in Tianwan Nuclear Power Plant. Probabilistic Safety Assessment and Management PSAM 12, June 2014, Honolulu, Hawaii