PSA-based Intelligent Design Suggestions for Nuclear Power Plant

WANG Ming*, ZHANG Bing, XIAO Lingmei, WU Yulong
China State Key Laboratory of Nuclear Power Safety Technology and Equipment, Shenzhen, China

Abstract: To enhance the safety of nuclear power plants through intelligent design, a systematic approach is proposed. This approach identifies suggestions for intelligent design to mitigate safety risks based on probabilistic safety analysis importance analysis results. Using the Level 1 PSA model for a typical Hua-long Pressurized Reactor (HPR 1000), recommendations for intelligent design improvements are offered. Analysis of specific cases show that by using some intelligent design for high importance items of nuclear power plant such as the fault diagnosis and health management (PHM) of the steam isolation valve in the secondary passive heat removal system (ASP), and the intelligent substation application to reduce the occurrence of Loss of offsite power (LOOP) may bring positive contributions to reduce safety risk.

Keywords: Intelligent design, Probabilistic safety analysis (PSA), Importance analysis, Nuclear power plant

1. INTRODUCTION

With the advancements in Industry 4.0 and the breakthroughs in new generation information technologies like artificial intelligence, internet of things, and cloud computing, intelligent design has become an inevitable trend in the development of nuclear power technology. It is a necessary means to enhance the safety, economy, and operational efficiency of nuclear power plants. Various intelligent designs such as data Twins nuclear power plant [1], predictive/preventive maintenance based on faults diagnosis and health management (PHM) system [2], intelligent control of operation procedure [3], and intelligent main control room [4] have been proposed and implemented in nuclear power plants. The concept of Smart Nuclear Power (SNP) introduced by nuclear power enterprises like China General Nuclear Power Corporation (CGN) has elevated the intelligence level of nuclear power plants through extensive digital and intelligent applications.

Despite the benefits, the input-output ratio poses a critical concern for designers and operators in the intelligent design of nuclear power plants. Unlike traditional nuclear power plants, the application of new intelligent or digital technologies in nuclear power plants, collectively referred to as intelligent design in this paper, requires adherence to stricter technical standards in the nuclear power sector and may necessitate specialized development. The nuclear power market's smaller scale and higher technology research and development costs present additional challenges compared to traditional industries. Moreover, while intelligent technologies may be technologically ready for implementation in nuclear power plants, excessive redesigning of structures, systems, and components (SSCs) can escalate engineering costs.

Probabilistic Safety Analysis (PSA) serves as a crucial tool for assessing the safety of nuclear power plants and forms the foundation of risk-informed technology, guiding the optimization of nuclear power plant designs. By identifying factors with "significant risks" to nuclear power plants through PSA results, appropriate intelligent design schemes can be selected to improve plant safety and enhance safety benefits. This study outlines a systematic methodology for identifying intelligent design recommendations to mitigate safety risks in nuclear power plants based on PSA findings, offering specific suggestions for intelligent design improvements based on the Internal Events Level 1 PSA model for a typical Hua-long Pressurized Reactor (HPR 1000). The research outcomes provide valuable insights for enhancing the intelligent design and optimization of nuclear power plants.

2. FORMDESIGN CONCEPT

As one of the important technical elements of PSA, importance analysis plays a significant role in identifying safety weaknesses, uncovering important risk factors, and suggesting ways to mitigate risks in nuclear power plants. This study proposes intelligent design recommendations based on the results of PSA importance analysis to reduce risks in nuclear power plants. The detailed implementation process is illustrated in Figure 1.

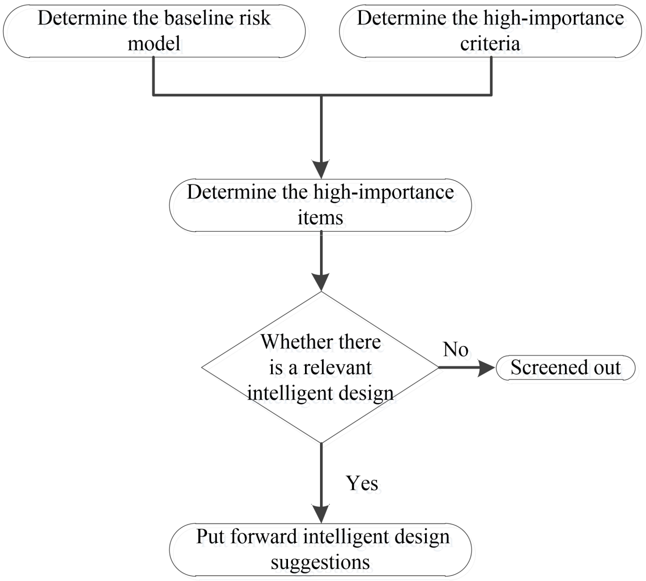
Determine the baseline risk model
Determine the high-importance criteria
Determine the high-importance items
Whether there is a relevant intelligent design
No
Screened out
Yes
Put forward intelligent design suggestions

Figure 1. Flow Chart Analyzing PSA-based Intelligent Design Suggestions

2.1. Determine the Baseline Risk Model

An appropriate PSA model can reduce the uncertainty of importance analysis results. When choosing a PSA model for importance analysis, specific selection principles need to be followed:

a) The baseline risk model should be highly accurate and preferably approved through regulation or peer review, for instance, the PSA model used in nuclear power plant licensing or the living PSA model for configuration risk management.
b) The design aspects in the risk model should align with those of nuclear power plants intending to incorporate intelligent designs, such as the consistent nuclear power technology.

2.2. Determine the High Importance Criteria

Fussel-Veseley (FV) importance and Risk Achievement Worth (RAW) are commonly utilized to assess the significance of modeled elements in risk-informed applications, which are defined as follows:

a) Importance *FVi* refers to the total frequencies of all minimum cut-sets (MCSs) that include basic event i, as a proportion of the total risk quantification value (such as Core Damage Frequency (CDF)). The formula for *FVi* is detailed in Equation (1). A higher *FVi* value indicates a more significant impact on the safety of nuclear power plants from random failures of basic events.

$$FV_{\mathrm{i}} = Q(\sum\nolimits_1^n MCS_i) / Q_b \tag{1}$$

Whereby,
MCS_i is the minimum cut-set that includes the basic event *i*,
Q stands for the total quantitative risk value of the nuclear power plant,
Q_b is the nuclear power plant benchmark quantitative risk value.

b) Risk enhancement value RAWi characterizes the increase in the total quantitative risk value if a basic event i has occurred (i.e., a basic event i is in the TRUE state), thus increasing the total quantitative risk value, it can be characterized by Formula (2). A higher RAW value indicates a stronger impact on safety caused by the random failure of the basic event.

$$RAW_{\mathrm{i}} = Q(P_i = 1) / Q_b \tag{2}$$

Whereby,
$P_i=1$ means the unavailability of basic event *i* is set to 1.

Referring to NEI 00-04 [6], the screening criteria for identifying high-importance items can be described as follows:

a) When the FV importance of an individual item exceeds 0.005, the total FV importance of all basic events (including related Common Cause Failure (CCF) events) is considered for high importance items.
b) Basic events with RAW greater than 2.

It should be noted that the above screening criteria are not applicable to the screening of high-importance initiating events. As a supplement to the above screening criteria, the *FV* importance of initiating events is greater than 0.01 as the screening criteria for high importance initiating events in this study based on engineering experience. In addition, the main purpose of importance analysis is to identify items that contribute significantly to risks. Therefore, when using this high importance initiating event screening criterion, if the component failure mode characterized by different initiating events is the same, these initiating events and their *FV* should be combined. For example, the Loss of Coolant Accident (LOCA) is usually divided into large LOCA, medium LOCA, and small LOCA based on the size of the pipeline break within the primary circuit boundary and the success criteria for accident mitigation in PSA model. However, these initiating events may all represent the same items (the pipe break within the primary circuit boundary). Therefore, when screening high importance initiating events, the *FVs* of these LOCAs should be merged before using the above high importance initiating event screening criteria for screening.

By quantifying the PSA model, the analysis calculates the importance of initiating events, component failure events, and human failure events (HFEs) separately. The rationality of these importance analysis results also needs analysis to identify uncertainties and recognize items with high risk contributions.

2.3. Identify Related Intelligent Design

Many intelligent design schemes applicable to nuclear power plants were not originally suggested to enhance safety. Instead, some were proposed from the perspective of improving operation and maintenance convenience, or improving the economics of nuclear power plant. That is, numerous intelligent design solutions are unrelated to safety enhancements.
Therefore, it is necessary to identify these intelligent design schemes after completing the recognition work of high importance items, and assess whether these intelligent designs are beneficial for,

a) Reduce the frequency of high importance initiating event or eliminate high importance initiating event.
b) Reduce the probability of high importance component failure event or eliminate high importance component failure event.
c) Reduce the probability of high importance HFE or eliminate high importance HFE.

2.4. Put Forward Intelligent Design Suggestions

Priority consideration should be given to identified high importance items in intelligent design schemes aimed at enhancing nuclear power plant safety. By prioritizing these items, the expected intelligent design goals can be met while maximizing safety benefits. For instance, advanced monitoring methods may be employed to track the performance and predict the future status of crucial valves, enabling proactive intervention to prevent unplanned shutdowns. When selecting valves for implementation of this intelligent design, those identified as of high importance should take precedence.

3. CASE ANALYSIS

3.1. Case Description

The study selects the Internal Events Level 1 PSA model for a typical HPR 1000 nuclear power plant of CGN Group as an analysis case. HPR1000, a third-generation nuclear power technology developed independently by CGN, is characterized by 177 groups of fuel assembly core and a series of three isolated entities based on the world's highest safety requirements and the latest technical standards.

The selected PSA model is developed based on the requirements of ASME/ANS RA-Sb-2013 [7], power operation, low power operation and shutdown operation of nuclear power plant in considered. Data on component reliability involved in the model mainly refers to NUREG/CR-6928 [8] and Chinese equipment reliability data database [9]. In Human Reliability Analysis (HRA), the human reliability analysis program-accident sequence assessment (ASEP) [10] and standardized plant risk analysis-human reliability analysis (SPAR-H) [11] are used to estimate Human Error Probabilities (HEPs).

3.2. Importance Analysis Results

Considering the relatively large number of high importance items identified according to the screening criteria given in Section 2.2, to simplify the analysis, the following high importance items are chosen in this case.

a) The component failure events and HFEs with the top 5 importance contributions are selected in this case, as shown in Table 1 and Table 2 respectively.
b) Initiating events with FV exceeding 0.1 are shown in Table 3.

Table 1. High Importance Basic Events Related to Component Failure (Top 5)

Category	Sort	Code	Description	Rationality
FV	1	RGL_4	Stuck 4 or more control rods	The shutdown function serves as a critical safety measure in various accident scenarios, if fails due to stuck control rods will directly lead to Core Damage (CD) or Anticipated Transient Without Scram (ATWS), The latter still has a certain probability of causing CD.
	2	I&C-DIAI_KDS_AR-FT	Failure of Signal Acquisition and Distribution Cabinet (KDS)	This event models the gathering and dissemination of different signals like Steam Generator (SG) pressure, SG water level, pressurizer pressure, and others. Failure in signal acquisition and distribution leads to the automatic triggering failure of the relevant safety injection system, impacting the safety of the unit.
	3	LHP001APD_FR3-ALL	Common cause operation failure of Emergency Diesel Generators (EDGs)	If EDGs and SBO diesel generators malfunction, the accident mitigation systems powered by these generators cannot be activated following a Loss of Offsite Power (LOOP) event. As the mobile diesel engine is not modeled in the PSA model, conservative assumptions directly lead to CD.
	4	&RPC_4-ALL	CCF of 4 Reactor Protection Cabinets (RPC)	The CPU units in the RPC cabinets are mainly used for shutdown protection and Engineered Safety Features (ESFs) signals. A CCF of more than 3 CPU units will result in the inability to give shutdown signals or the inability of ESFs to start, affecting the start-up of post accident mitigation functions, thus making a certain contribution to the risk of the unit
	5	PGR	Failure of power grid restoration	Power grid restoration can provide power to systems and equipment used for accident mitigation in a LOOP accident.
RAW	1	ASP3110VVE_EL	Steam inlet motor isolation valve ASP3110VV external leakage	As a backup means, the Secondary Passive Heat Removal System (ASP) needs to continuously discharge the heat from the primary circuit after other secondary circuit cooling means fail. The cooling function of ASP will be affected due to steam inlet motor isolation valves external leakage.
	2	ASP1110VVE_EL	Steam inlet motor isolation valve ASP1110VV external leakage	
	3	ASP21110VVE_EL	Steam inlet motor isolation valve ASP2110VV external leakage	
	4	RGL_4	Stuck 4 or more control	Consistent with the same event mentioned in the FV

			rods	above.
	5	LHA1101TBF_FW	Failure of distribution panel LHA1101TB operation	If the LHA1101TB distribution panel fails to operate after LOOP occurs, the mitigation systems driven by the electrical cabinet cannot be put into use. The model assumes that it directly causes CD.

Table 2. High Importance Human Failure Events (Top 5)

Category	Sort	Code	Description	Rationality
FV	1	OP_LHSI_HC1	Failure of simultaneous injection operation in cold leg and hot leg of low pressure safety injection system	The long-term stage of large/medium LOCA, operators need to perform simultaneous injection of cold leg and hot leg to avoid boron crystallization on the fuel and causing local high temperatures. This basic event is used in multiple LOCA event trees and has a high frequency of LOCA initiating events, thus making a significant contribution to risk.
	2	OP_ASG1_LINK	Failed to manually connect Auxiliary Feedwater System (ASG) tanks in other columns (columns 2 and 3)	This HFE resulted in a failure of ASG column 1, reducing the reliability of ASG. A corresponding fault tree is used in multiple functional events, and nearly 30 event trees modeled the water replenishment function of ASG.
	3	OP_ASG2_LINK	Failed to manually connect Auxiliary ASG tanks in other columns (columns 1 and 3)	
	4	OP_SBO	Failed to manually start up Station Blackout (SBO) diesel generators	If SBO diesel generators fail to be manually started up after LOOP occurring and EDGs fail, all mitigation systems driven by diesel generators cannot be put into use. As the mobile diesel engine is not modeled in the PSA model, adhering to the assumption directly leads to CD.
	5	OP_RHR_S	Failed to manually re-start up Residual Heat Removal (RHR) pump	When a small LOCA occurs and requires the restoration of residual heat removal mode to fail in low power operation stage, the RHR pump requires to be restarted manually to remove residual heat from the core, otherwise it may cause CD.
RAW	1	OP_LHSI_HC1	Failure of simultaneous injection operation in cold leg and hot leg of low pressure safety injection system	Consistent with the same event mentioned in the FV above.
	2	OP_ISO_DIL	Failed to manually isolate dilution source or implement corrective action in case of successfully carry out Extra Borating System (RBS)	In a boron dilution incident, manual isolation of the dilution source is a backup means to correct the failure of the automatic isolation of the false dilution source, preventing excessive dilution in the primary circuit from causing supercritical conditions.
	3	OP_RHR_S	Failed to manually re-start up Residual Heat Removal (RHR) pump	Consistent with the same event mentioned in the FV above.
	4	OP_IRWST_S	Failed to manually switch to Containment Heat Removal System (EHR)	As a backup means, EHR cooling need to be switched manually after the failure of other cooling means for In-containment Refueling Water Storage (IRWST).
	5	OP_ASG1_LINK	Failed to manually connect ASG tanks in other columns (columns 2 and 3)	Consistent with the same event mentioned in the FV above.

Table 3. Initial Events with FV greater than 0.1

Sort	Code	Description	Related Equipment/Facilities	Rationality
1	LOCA	Large, medium and small breaks in primary circuit	Pipeline within the pressure boundary of primary circuit	Both the frequencies of initiating events and the probabilities of failing accident mitigation measures are relatively high.
2	LOOP	Loss of power outside the plant	power grid, main transformer voltage transformer, auxiliary Transformer, overhead lines, etc.	

3.3. Suggestions for Intelligent Design

By identifying high importance information in Section 2.2 and integrating it with relevant intelligent design schemes focusing on the CGN SNP project, the following intelligent design recommendations can be made.

a) Include high importance equipment like ASP3110VV/ASP1110VV/ASP2110VV and LHA1101TB in the intelligent design scope. Monitor the operation status of these equipment, assess their performance, and use intelligent algorithms to predict future status and performance. Take proactive maintenance measures to mitigate safety risks from equipment failures during unit operation.
b) Prioritize optimizing high importance HFEs in accident operating procedures automation scheme. Examples include failure of simultaneous injection operation in cold and hot legs of the low-pressure safety injection system and manual connection to other ASG water tanks. Utilize group control and automatic diagnosis technologies to simplify or eliminate the complexity of these HFEs.
c) Implement advanced measurement technologies such as fiber optic sensors and digital instruments to enhance signal acquisition and transmission reliability.
d) Intelligent design proposals that can reduce the frequency of LOOP initiating events should be given priority consideration, such as the technology of smart substations. By leveraging automated control systems to continuously monitor electric power quality data and faults, and responding promptly to abnormal conditions, these designs minimize human errors and operational delays. Consequently, this enhances the stability and reliability of the power grid.

In addition to the high importance items mentioned in the suggestions above, there are other high importance items (such as common failures in the operation of EDGs, stuck control rods, etc.). Since intelligent design schemes that can mitigate their safety risks have not yet been implemented, specific intelligent design suggestions have not been proposed. However, it is advisable for the intelligent design team to continue focusing on these high importance items during the intelligent design process. If there are intelligent design solutions that can reduce these high importance items in the future, they should be prioritized.

3. CONCLUSION

This study exemplifies the application of risk-informed technology in optimizing the design of nuclear power plants. It accurately identifies "significant risk" factors to assist the intelligent design team in making decisions that enhance the safety and benefits of nuclear power plants in design activities. During the utilization of the methodology to guide the intelligent design of nuclear power plants, the following aspects are suggested for consideration.

a) For the determination of the object of intelligent design, from the perspective of safety contribution is only an auxiliary means. The intelligent suggestions proposed from the perspective of PSA also need to consider additional factors such as component failure mechanism and historical operating experience, and ultimately form a specific scheme that can be implemented.
b) The screening criteria in this study may identify a large number of highly important items. Designing intelligence for all these items is impractical. Hence, stricter screening criteria can be established, similar to those in the preceding case analysis, to focus on specific high importance items during the intelligent design process.
c) Emphasis should be placed on understanding the impact of uncertainty in importance analysis results. Uncertainty sources include model integrity and data uncertainty. For instance, baseline risk model analysis results may not accurately represent the characteristics of the target nuclear power plant, and some intelligent design technologies may not be accounted for in the PSA model.

d) The high importance screening criteria proposed in this study are only applicable to internal event PSA, while for intelligent design optimization suggestions related to external event risk, new screening criteria may need to be re-determined based on the conservatism of external event risk model and analysis boundary.

e) The intelligent design of nuclear power plants based on PSA can be a continuously iterative process. After identifying the intelligent design features to be implemented, these new characteristics can be updated within the PSA model. Based on the quantitative results of the updated PSA model, newly identified significant risk factors can be assessed, and further recommendations for intelligent design can be proposed.

Acknowledgement

Thanks to the National Key Laboratory of Nuclear Power Safety Technology and Equipment and the SNP project of CGN for their financial and technical support.

References

[1] Huang Jianhua and Guo Tianjue. Development and application of intelligent nuclear power plant. China Nuclear Power, 14, 138-143, 2021.

[2] Hu Y, Miao X, Si Y, et al. Prognostics and health management: A review from the perspectives of design, development and decision. Reliability Engineering and System Safety, 217, 108063, 2021.

[3] JaeKwan Park, TaekKyu Kim, et al. Control automation in the heat-up mode of a nuclear power plant using reinforcement learning. Progress in Nuclear Energy, 145, 104107, 2022.

[4] Morita, Akane, Komatsubara, Tadao, et al. Intelligent main control room for advanced PWR plants. Mitsubishi Juko Giho, 35, 258-261, 1998.

[5] Guo Jingren. Solutions and Applications of SNP. China Nuclear Industry, 6, 23-24, 2019.

[6] Nuclear Energy Institute. 10 CFR 50.69 SSC Categorization Guideline, NEI 00-04, Rev. 0, Washington, DC, 2005.

[7] ASME/ANS. Addenda to ASME/ANS RA-S-2008, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME/ANS RA-Sb-2013, The American Society of Mechanical Engineers & American Nuclear Society, New York, U.S., 2013.

[8] NRC. Industry-average performance for components and initiating events at U.S. Commercial nuclear power plants, NUREG/CR-6928, Washington, DC, 2015.

[9] National Nuclear Safety Administration. Report on Equipment Reliability of Chinese Nuclear Power Plants, General Office of Ministry of Ecology and Environment of the data, Beijing, 2016.

[10] NRC. Accident sequence evaluation program human reliability analysis procedure, NUREG/CR-4772, Washington, DC, 1987.

[11] NRC. The SPAR-H human reliability analysis method, NUREG/CR-6883, Washington, DC, 2005.