Risk-Informed Design Changes of an Advanced Reactor in Low Power and Shutdown Operation

Ji-Yong Oh*[a], Ho-Rim Moon[a], Han-Gon Kim[a] and Myung-Ki Kim[a]

[a] Korea Hydro and Nuclear Power Co. Ltd, Central Research Institute, Deajeon, Korea

Abstract: APR+ has been developed in Korea since 2007. APR+ adopts various advanced safety features including passive auxiliary feedwater system, four emergency diesel generators. Through the implementation of the advanced designs, APR+ increased the safety to the world best level of evolutionary reactors. The full power core damage frequency or containment failure frequency decreased significantly comparing to APR1400 that is base model of APR+. However, low-power shutdown risk has not been improved substantially. This paper suggests several design changes that optimize low-power shutdown risk. Based on the design alternatives, this paper discusses risk effectiveness of the proposed design including various factors, e.g. equipment reliability, human error, training, procedure and so on.

Keywords: PRA, LPSD, Mid-loop, SDC

1. INTRODUCTION

Before 1980s, people in nuclear industry believed that the level of reactor decay heat during low power and shutdown (LPSD) state is very low comparing to the case of normal operation mode. People also believed that operator could have enough time to manage the accident in LPSD state so that the associated risk might not be significant and might be ignorable in comparison with full power state. In 1987, Diablo canyon nuclear power plant experience the accident that result from the loss of residual heat removal function during mid-loop operation. The industry and regulatory had focused on the safety issue for the shutdown sate, particularly the hazard on mid-loop operation. Nuclear Regulatory Commission (NRC) had investigated the accident in Diablo canyon and inspected the readiness of the same kind of accident for other plants in the U.S. The industry and NRC investigation resulted that the decay heat level might not be so small and the available resources of safety systems during LPSD might not be sufficient so that the associated risk for LPSD would not be ignorable comparing to that of full power. On the following, NRC issued a generic letter [1] urging the industries to implement the expeditious actions as well as programmed enhancements for LPSD. On the risk perspective, the industry provided the guidance [2] for industry actions to assess shutdown management.

The APR+ design adopts various advanced safety features including passive auxiliary feedwater system, four emergency diesel generators, rigorous containment design preparing for aircraft impact, and so on. Particularly, the design has four independent trains separating with the concept of mechanical, electrical and physical. Note that these four independent features enable the APR+ design to implement on-line maintenance with an effective manner. Through the implementation of the advanced features, the risk level of APR+ design for full power is the world best level of evolutionary reactors. However, in terms of LPSD, the efforts improving the safety have not been made a prominent progress during the stage of standard design approval [3]. In order to reduce the overall risk associated with all modes and all hazards, the appropriate process or method should be developed to deal with the LPSD risk.

This paper discusses the LPSD risk of the APR+ design. First, the characteristics of LPSD risk are presented including the concept of plant operational state, mid-loop operation, and special initiating events in section 2. In section 3, a new process is proposed to identify the design alternatives

* Corresponding Author, teslar@khnp.co.kr

improving LPSD risk. This process also performs the conceptual level designs for the alternatives. Moreover, the sensitivity analyses associated with the design alternatives are evaluated and the best design option is determined based on the process. In conclusion, this paper discusses the positive and negative effect when the proposed design is implemented.

2. CHARACTERISTICS OF LOW POWER SHUTDOWN RIKS

2.1. Plant Operational State (POS) Definition

According to the continuously changing plant configuration in any outage, plant operational states (POSs) are defined and characterized. Each POS represents a unique set of operating conditions (e.g., temperature, pressure, and configuration). For the typical refueling outage of PWR, up to 15 POSs are usually used, representing the evolution of the plant throughout a refueling from low power down to cold shutdown and refueling, and back-up to low power [4].

The LPSD risk model associated with APR+ design adopts 15 POSs including two more sub states in POS 4, 10. The 17 POSs are divided based on six operating modes in technical specification, reactor coolant system (RCS) water level, RCS opening (pressurizer manway, SG manway), active core in reactor, and maintenance schedule of main safety systems and supporting systems. Plant configurations of POS 1,2,14 and 15 are the same as these of full power and POS 5, 11 are correspond to mid-loop operation. POS 7, 8 are associated with fuel loading and reloading. The durations of POSs are referencing to the outage practice of Shin-Gori 3&4 plant [5].

2.2. Mid-Loop Operation

In mid-loop operation mode, operators decrease RCS level to mid-level of hot leg to install SG nozzle dams and replace seal or journal bearing of reactor coolant pumps. After that, operators increase RCS level up to the top of hot leg. Through the mid-loop operation, SG eddy current test (ECT) or maintenance work can be performed in parallel with core alteration so that the significant amount of the outage time can be save impacting on the plant economies.

On the contrary, RCS level is too low and its associated time to boil or core uncover is also very short that caused relatively high risk state during mid-loop operation. Particularly, the loss of shutdown cooling function during mid-loop is one of the most vulnerable events that some evolutionary plants have experienced. In addition, during outage including mid-loop, the available critical safety functions can be limited, for instance SGs and some safety injection pumps may not be available after RCS is drained and breakers are racked-out for the purpose of preventing inadvertent injections. In general, mid-loop operation is the most important stated during LPSD on the perspective of risk so that the cautious RCS level control as well as the continuous monitoring of shutdown cooling function are essential in this operating.

2.3. Initiating Event for Low Power Shutdown Operation

NUREG/CR-6144 [4] documented a shutdown PRA for Surry Unit 1 in 1994. It provided a sound analysis of a comprehensive set of initiating events and then-current data. LPSD risk model of APR+ adopts NUREG/CR-6144 [4] as the basis of initiating event. In addition to that, Standard Safety Analysis Report (SSAR) [6] of APR+, specifically LPSD parts and the PSA report of Sin-Kori 3&4 [5] are reviewed to identify LPSD initiating events.

There are two major categories for IE, i.e. Loss of Coolant Accidents (LOCAs) and transient events. LOCAs are divided into more detailed levels, i.e. unrecoverable LOCA (CVCS letdown line), LTOP safety valves fails to reclose, and so on. The categories of transients are almost the same as that of full power mode. The loss of shutdown cooling (LOSC) is one of LPSD specific initiators and the most

important risk contributors in LPSD operation modes. LOSC is divided into four sub-level categories as following:

- S1 - Recoverable Loss of Shutdown Cooling System
- S2 - Unrecoverable Loss of Shutdown Cooling System
- SO – Over-drainage during Reduced inventory Operation
- SL – Failure to Maintain Water Level during Reduced Inventory Operation

The former two IEs are initiated by the mechanical failure of shutdown cooling (SCP) and the latter two IEs are caused by SCPs failure due to the cavitation by insufficient suctions. The most dominant IE during LPSD is over-drainage during reduced inventory operation, which results from inadequate level control of operators or the failure of level instruments.

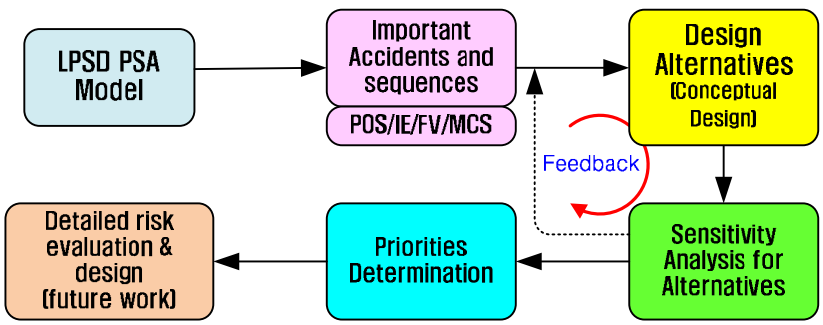
3. DESIGN ALTERNATIVES

The design alternatives are identified by the overall process that is developed in this paper. The overall process uses the LPSD PSA model of APR+ design and identifies the design alternatives that provide additional safety functions and prevent plausible accidents during LPSD operation modes. Conceptual designs for the alternatives are performed and the design effectiveness is evaluated by the sensitivity analysis with the associated risk parameters. With the outcome for the alternatives, the priorities are determined with a comprehensive evaluation considering the negative influences for other areas.

3.1. Overall Process

In order to identify appropriate design alternatives that possibly minimize LPSD risk, developing stage PRA model of APR+ and its results, for instance CDF lists depending on POS and IE, the importance values, minimal cutsets (MCSs) are used [7]. In the first step, important operational mode, accidents and accident mitigation functions are identified by reviewing CDF lists for POSs, IEs and importance values. Important sequences are discussed with the MCS analysis of APR+ design. In the second step, the preventive measures and design alternatives are elicited based on the result of the first step. The conceptual designs for the alternatives are performed with the cooperation of risk analyst and system and component designers. Specifically, the interpretation of MCSs identifying the importance accident sequences on the stand point of risk and the findings of their remedial measures are very important in this step. The third step evaluates the effectiveness for the proposed design alternatives through the sensitivity analysis of associated risk parameters. The purpose of this step is not to obtain explicit risk value but to acquire the risk insights from the proposed designs. Therefore, more comprehensive interpretation should be done in the determination of risk parameters. In the fourth step, the priorities are determined and the negative influences are discussed with more comprehensive perspectives including industrial safeties, licensing issues and design varying controls. The final alternative selected by the former steps proceeds to the detailed design and risk evaluation step. Particularly, an iterative process is carried out throughout the first step and the third step in the process. The actual applications of the process are implemented with APR+ design in the followings.

Figure 1: Design Optimization Process for LPSD risk



3.2. POS/IE/Importance/MCS analysis

The result of LPSD PRA for the APR+ shows that the most risk values are concentrated on the mid-loop and associated drain operation that correspond to POS 5&11 (mid-loop), and POS 4B&10 (drain operation). POS 5&11 and POS 4B&10 take 55.9% and 23.9% portions of the total LPSD CDF, respectively. Particularly, POS 5 (first mid-loop operation) takes 44.8% of the total LPSD CDF and identified as the most vulnerable operation state in LPSD.

In terms of the LPSD initiating events, SO (over drain), S1 (recoverable SCP fail) and S2 (unrecoverable SCP fail) are dominant and take 28.3%, 18.7% and 14.4% portions of the total LPSD CDF. These events categorizing the loss of shutdown cooling are major initiating events that lead to core damage with high frequencies. Except these kinds of IEs, the noticeable events are the loss of component cooling water, station block out, and stuck open of pilot operated safety relief valves. Particularly, some of AC sources e.g. EDG, UAT, and SAT might not be available even in the mid-loop operations since the component maintenance activities.

With the view of the importance analysis, the SO initiating event has the highest value of Fussel-Vessely (FV) [8] where the events contribute to the system reliability. Following the events, the common caused failure (CCF) of essential chillers, sump plugging event under feed & bleed operation, and operator action to RCS inventory recover ranks the top four of the FV values. The events associated with high importance event, e.g. dependent events are ranked high in the FV lists.

In the MCS analysis, the most probable sequence is occurred in POS5 and the sequence takes 13% portion of the total LPSD CDF. The sequence can be demonstrated by the following detailed scenario description. During the start of mid-loop operation, operator errors or level indication failures lead to the loss of shutdown cooling. Operator actions for recovering RCS inventory using available SCPs are attempted but failed. And then, Operators tried to feed & bleed operation using the available safety injection pumps. When the trial also failed, operators attempted the feed Y steaming operation using the charging pumps. All these mitigation systems with associated operator actions are failed sequentially and finally the core reached the success criterion temperature of CDF. The scenario of the second high sequence is similar to that of the first one except the initiating event and first mitigation action. The sequence is also occurred in POS5 with the recoverable SCP fail and operators attempt to recover SCP as the first mitigation action but failed. The other progress is pretty similar to that of the first one. The combination events of the loss of shutdown cooling and CCF of essential chillers (WOCHKQ4) are shown in the high rank MCS. In case of WOCHKQ4 leads to core damage with a simple combination with several initiating events, representing that the common caused failure of safety injection system might become a very critical event with some IEs in the several POSs.

Table 1: Minimal Cutset for APR+ LPSD

Rank	Mean		Minimal Cutset			
	(/year)	(%)				
1	3.58E-07	13	%SOP05	HR-FB-SOP05-02-DE	HR-FS-SOP05-02-DE2	HR-MK-SOP05
2	2.03E-07	7.4	%S1P05	HR-FB-S1P05	HR-FS-S1P05-DE	HR-RS-S1P05
3	1.48E-07	5.4	%SOP11	HR-FB-SOP11-02-DE	HR-FS-SOP11-02-DE2	HR-MK-SOP11
4	1.25E-07	4.5	%S2P05	HR-FB-S2P05	HR-FS-S2P05-DE	HR-RS-S2P05
5	8.73E-08	3.2	%CCP05	HR-FB-CCP05	HR-FS-CCP05-DE	HR-RS-CCP05
6	7.97E-08	2.9	%PLP02	WOCHKQ4-CH01A/B/C/D		
7	7.86E-08	2.8	%S1P05	HR-FS-S1P05	HR-RS-S1P05	SISPP-P456
8	6.13E-08	2.2	%LPP10	WOCHWQ4-CH01A/B/C/D		
9	4.85E-08	1.8	%S2P05	HR-FS-S2P05	HR-RS-S2P05	SISPP-P456
10	4.79E-08	1.7	%SOP05	WOCHKQ4-CH01A/B/C/D		
11	4.79E-08	1.7	%SOP11	WOCHKQ4-CH01A/B/C/D		
12	4.53E-08	1.6	%S1P10	WOCHKQ4-CH01A/B/C/D		

※ SO : loss of SCP due to over drain , HR-: human action, WOCHWQ4 : CCF of essential chillers
S1 : recoverable SCP mechanical random fail , F&B : feed & bleed, F&S : feed & steaming
S2 : unrecoverable SCP mechanical random fail

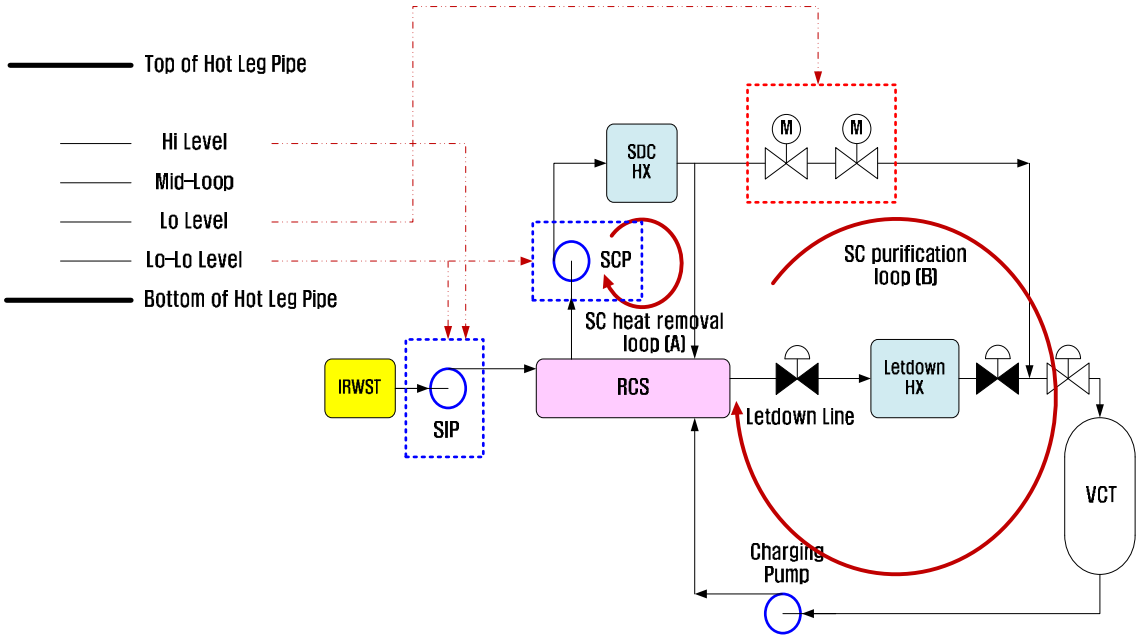
Through the risk analysis depending on POSs, IEs, importance, and MCSs, three design alternatives are identified. The first alternative is associated with the prevention of the initiating event caused by the loss of shutdown cooling including over drain (SO) and failure of maintain water level (SL). The second alternative is corresponds to the reliability enhancement for the operator manual actions in feed and bleed operation (HR-FB-**). An alternative design is proposed with automated injections by hot leg level signal. In the third alternative, an alternative associating with the diverse function for room cooling of safety pumps is elicited. By the implementation of the alternative, the probability of essential chiller CCF can be mitigated. The first and second design alternatives are applied to only LPSD operations. However, the third item is applicable to both full power and LPSD. Since the various safety functions my not be available due to the maintenance, the CCF of essential chiller would be critical during LPSD.

3.3. Design Alternatives

3.3.1. Prevention of loss of shutdown cooling (alternative 1)

RCS levels during mid-loop operation are controlled and balanced by shutdown cooling system (SCS) and chemical & volume control system (CVCS). The heat removal loop (loop A in figure 2) is established by shutdown cooling system with a closed loop shape. The purification loop (loop B in figure 2) starts from the discharge line of shutdown cooling (SDC) heat exchanger (HX) and connected to volume control tank (VCT) of CVCS. In order to prevent over drain or inadvertent level loss during mid-loop, the first design alternative is proposed with the installment of automatic isolation of MOVs (red dot line in figure 2) in the purification line when RCS level decrease to Lo level (figure 2). The design corresponding level sensors, signal transmitters and logic devices are included in the alternative. This design prevents the RCS inventory loss during the accident with an automated manner. Through the implementation of the design alternative, the initiating event associated with over drain or failure of maintain water level can be significantly reduced.

Figure 2: Design alternative 1&2 for reducing LPSD Risk (Automatic purification line isolation and SIP injection)



3.3.2. Automated safety injection under RCS level reduced (alternative 2)

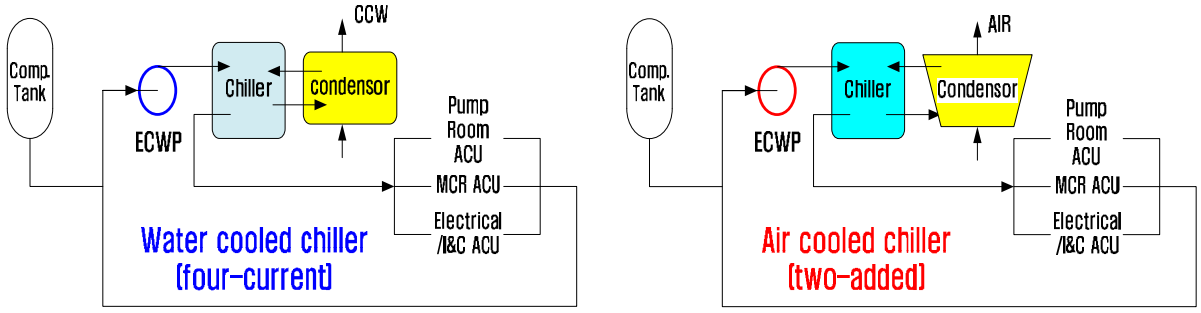
When an event associating with over drain (SO) and failure of maintain water level (SL) is initiated, immediate action to stop the running SCP and to start safety injection pumps (blue dot line in figure 2) should be taken to mitigate the accident. The second design alternative automates the injections by the level signal from hot leg. When RCS level decreases continuously below Lo level and reaches Lo-Lo level, the automated systems are activated. When RCS level is recovered to Lo level, SCP starts again. If RCS level reaches Hi level, then a signal to stop the safety injection pumps are transmitted. The design corresponding level sensors, signal transmitters and logic devices are included in the alternative. In addition, the hot leg level should be set for generating the relevant signals, e.g. Lo-Lo, Lo, Hi level (figure 2).

3.3.3. Diversified room cooling for safety systems (alternative 3)

The essential chillers provide chilled water to the regional cubicle coolers that remove heat from safety class equipment room ensuring equipment survivability under the accidents. APR+ design adopts four trains of essential chilled water (ECW) system and each train has 100% heat removal capacity. The removed heat is transferred to the component cooling water (CCW) system in the heat exchangers of the condenser, and another heat removal cycle, essential service water (ESW) system is connected to CCW system. Therefore, the loss of ultimate heat sink or common caused failures of CCW/ESW components result in the function loss of the ECW system. Eventually, these all series events lead to the function loss of safety systems and components that require heat removal during the accident.

The basic event, WOCHKQ4 in MCS represents CCF event of four essential chillers. In order to break the common caused failure mode, the third alternative proposes the diversification in the design of ECW and its supporting systems. First, two additional ECWs are introduced, which use different types or different manufacturers from the original pumps, chillers. And next, the added ECWs are introduced the heat sink as air-cooled type while the original ECWs use water-cooled type. Through these two diversified designs, risk associated with LPSD operation mode would be significantly reduced.

Figure 3: Design alternatives for reducing LPSD Risk
(Additional chilled water systems using air condensing)



3.4. Sensitivity Analysis for Design Alternatives

Sensitivity analysis is used to evaluate the effectiveness of the proposed design alternatives with the associated parameters. The detailed modeling and risk analysis will be performed in the fifth step. The case studies for sensitivity analysis are performed changing the associated risk parameters with the factor of 0%, 10%, 50%, and 100%. The changes of core damage frequencies are measured depending on the factored values and the effectiveness of the design alternatives are interpreted based on the result of the sensitivity analysis. The combination effect of the first and second alternatives is evaluated as well.

First, the risk parameters are designated for the sensitivity analysis. In the first alternative, the initiating event of over drain during mid-loop operation, POS 5 and POS11 is selected as the representative risk parameter. And the second alternative chooses the basic events for the operator actions associated with feed and bleed operation during accident mitigation. The common caused failure event of essential chillers is designated as the representative risk parameter.

Second, the effectiveness is measured for the case of 0%, 10%, 50%, and 100% sensitivities. In terms of the first alternative, when the risk parameter is factored to 10%, the total LPSD CDF is reduced to 25%. The selected parameters are mainly effective for POS 5 and POS 11, mid-loop operation. For the second alternative, automated design of safety injection, when the risk parameter is factored to 10%, the total LPSD CDF is reduced to 34%. The selected parameters are associated with operator action for feed & bleed. For more efficient work process, the operational state and applicable cutsets are limited to 5&6 and the top 100. The top 100 cutsets cover almost 90% of the total LPSD CDF so, the simplified application would be sufficient to identify the effectiveness of the alternatives and obtain the associated risk insights. In terms of the combination alternative (1&2), when the risk parameters are factored to 10%, the total LPSD CDF is reduced to 43% from its original value. For the third alternative, when the probability value for the essential chiller CCF is factored to 10%, the total LPSD CDF is reduced to 14%. Although the risk parameter may not represent the whole design alternatives and the exact value can be evaluated with detailed design and modeling, the effectiveness for the alternatives can be estimated roughly with simple parameter sensitivity analysis.

In this paper, the maximum and minimum of the effectiveness are predicted by the result of 0% and 10% sensitivity cases. When a design alternative is implemented with very effective manners, the associated frequency or probability parameter would be reduced to very low value, e.g. $10^{-7} \sim 10^{-8}$ or even close to zero with optimistic perspectives. However, when the design alternative is poorly implemented, the gain from associated frequency or probability parameter would not be more than 10% with pessimistic perspective. These are the basis of qualitative assessment for the design alternatives and associated engineering judgments are included.

Table 2: Risk Sensitivity Analysis for the Design Alternatives

Alternative	Description	Risk Parameter	Sensitivity	Value	Total CDF (/yr)	CDF Reduction	Effectiveness (qualitative)
1	Prevention to Loss of Shutdown Cooling	%SOP05 %SOP11	100%	1.77E-03	2.76E-06	0%	High
			50%	8.87E-04	2.37E-06	14%	
			10%	1.77E-04	2.06E-06	25%	
			0%	0.00E+00	1.98E-06	28%	
2	Automated Safety Injection	HR-FB-** (POS 5&11)	100%	-	2.76E-06	0%	High+
			50%	-	2.35E-06	15%	
			10%	-	1.81E-06	34%	
			0%	-	1.70E-06	38%	
1+2	Alternative 1 + Alternative 2	%SOP05 %SOP11 HR-FB-** (POS 5&11)	100%	-	2.76E-06	0%	High++
			50%	-	2.05E-06	26%	
			10%	-	1.58E-06	43%	
			0%	-	1.52E-06	45%	
3	Diversify Room Cooling for Safety System	WOCHWQ4	100%	2.70E-05	2.76E-06	0%	Medium
			50%	1.35E-05	2.55E-06	8%	
			10%	2.70E-06	2.38E-06	14%	
			0%	0.00E+00	2.34E-06	15%	

3.5. Priority Determination

The result of the sensitivity parameter shows that the most effective alternatives are the case of combination 1&2. And next followings are the second alternative, the first alternative, and the third alternative. In the process of priority determination, not only the effectiveness of risk reduction but also other negative effects should be considered with more comprehensive manners. For instance, when the second alternative is implemented, there are possibilities for the faulted level sensing or unstable RCS level that triggers unexpected safety injection resulting in the radioactive contamination for the workers who are installing nozzle dam during mid-loop operation. As for the third alternative, although the design itself is simple to implementation, the added equipment and systems requires new space so that general arraignment should be changed and relevant additional seismic analysis should be performed. Moreover, if the design status is almost complete, the other associated design changes should be considered, e.g. HVAC configuration, new drawings for piping. On the more comprehensive perspective with risk evaluation, design, licensing, industrial safety, and constructability, the implementation of the first design alternative would be the best solution for APR+ design and the alternative plan proceeds to the fifth step.

4. CONCLUSION

This paper proposes three design alternatives to reduce low power shutdown risk for APR+ design. In order to determine the best alternative, risk parameters associated with each alternative have been identified and the corresponding conceptual designs are performed. The sensitivity analysis has been performed to measure the effectiveness of the proposed alternatives. Accordingly, comprehensive evaluations considering the negative effect of the design alternatives including design, licensing, and industrial safety has been done in the priority determination step. A best resolution has been determined and progressed to the next step.

As for the future work, the fifth step will be implemented including the detailed design and risk evaluation for the selected best alternative. Finally the completed work will be delivered to the construction phase of APR+ design.

References

[1] USNRC GENERIC LETTER NO. 88-17, Loss of Decay Heat Removal, October 17, 1988.
[2] NUMARC 91-06, “Guideline for Industry Actions to Assess Shutdown Management,” December 1991.
[3] KHNP, “APR+ Probabilistic Safety Assessment Technical Report,” June, 2011.
[4] USNRC NUREG/CR-6144, “Evaluation of Potential Severe Accidents during Low Power and Shutdown Operations at Surry, Unit 1,” October, 1995.
[5] KHNP, “APR1400 Probabilistic Safety Assessment for Low Power and Shutdown Operations,” January, 2012.
[6] KHNP, “APR+ Final Safety Analysis Report,” January, 2012.
[7] J. Oh, et al. “Risk Assessment and Safety Improvement for Low Power Shutdown Operation in Advanced Nuclear Power”, *Proceedings of KSME Reliability*, 2014, p5.
[8] Mohammad Modarres, “Reliability Engineering and Risk Analysis,” Marcel Dekker, 1999, New York.