Probabilistic analysis on the failure of reactivity control for the PWR

D T Sony Tjahyani, Deswandri, G R Sunaryo
Center for Nuclear Reactor Technology and Safety, BATAN Puspiptek Complex, Building no. 80, Serpong, Tangerang Selatan 15310, Indonesia
dtsony@batan.go.id

Abstract. The fundamental safety function of the power reactor is to control reactivity, to remove heat from the reactor, and to confine radioactive material. The safety analysis is used to ensure that each parameter is fulfilled during the design and is done by deterministic and probabilistic method. The analysis of reactivity control is important to be done because it will affect the other of fundamental safety functions. The purpose of this research is to determine the failure probability of the reactivity control and its failure contribution on a PWR design. The analysis is carried out by determining intermediate events, which cause the failure of reactivity control. Furthermore, the basic event is determined by deductive method using the fault tree analysis. The AP1000 is used as the object of research. The probability data of component failure or human error, which is used in the analysis, is collected from IAEA, Westinghouse, NRC and other published documents. The results show that there are six intermediate events, which can cause the failure of the reactivity control. These intermediate events are uncontrolled rod bank withdrawal at low power or full power, malfunction of boron dilution, misalignment of control rod withdrawal, malfunction of improper position of fuel assembly and ejection of control rod. The failure probability of reactivity control is 1.49E-03 per year. The causes of failures which are affected by human factor are boron dilution, misalignment of control rod withdrawal and malfunction of improper position for fuel assembly. Based on the assessment, it is concluded that the failure probability of reactivity control on the PWR is still within the IAEA criteria.

Keywords: Fundamental safety function, Probabilistic, Safety analysis, Reactivity control, PWR

1. Introduction
Safety assessment on the power reactor in accordance with international and national regulation is carried out by the probabilistic and deterministic analysis to obtain the site permit, as well as other permits especially the construction and operation permits [1]. The safety analysis is initiated by constructing event sequences with the purpose to determine initiating events and mitigation system consisting of safety system and operator actions. The mitigation system is required to overcome the initiating event, so that the core damage is not occurred [2]. Therefore, the safety analysis especially the probabilistic analysis, is important to analyze the frequency or probability of the initiating event and the failure of mitigation system. Hereinafter, the possibility of the occurrence of core damage can be determined. Based on this analysis, the safety design level of the power reactor can be evaluated.
The initiating event is determined by five group initiating events, which are used to evaluate the fundamental safety functions of reactivity control, heat removal from the reactor or the fuel storage, and confinement of the radioactive materials as also radiation shielding. To control operation, the important parameter considered is to control reactivity for all operating conditions and it needs to be analyzed. On the light water reactor, the reactivity control is the first stage for preventing the occurrence of core damage or the more severe accident propagation.

At present, the pressurized water reactor (PWR) is a type of nuclear power plants, which are operated mostly in the world. The Advanced Passive Pressurized Water Reactor 1000 (AP1000) is one of PWR type, that applies absolutely passive system on the passive core cooling system (PXS) with high reliability [3, 4]. Therefore, it is important to analyze the characteristic of AP1000 from the aspect of reactivity control.

The analysis indicated that neutronic characteristics more important than the thermal hydraulic characteristic at the beginning cycle of operation [5]. Also in general, the level 1 of probabilistic safety assessment (PSA) results showed that human action and dependent failures had significant effect on accident and its consequences [6]. The control rod as part of the reactivity control system might experience deterioration, which results in a stuck control rod or in advertent control rod drop [7]. Reactivity initiated accidents (RIAs), which cover a sudden and rapid control rod insertion, comprise the positive and negative reactivity [8]. The rod drop accident is an important event of RIA in LWR safety analysis, because this case can cause its adjacent regional power to increase rapidly and also the increase of fuel enthalpy [9]. Based on these researches, it showed that the reactivity control was generally carried out by deterministic analysis for the rod drop event. Therefore, it is very important to analyze the reactivity control from the several view points such as the mechanical failure, the human error, the procedure error and the others.

The purpose of this paper is to analyze the failure probability of the reactivity control and to determine the failure contributions, which cause the occurrence of the reactivity control failure in AP1000. The analysis is done by using deductive analysis, which is fault tree analysis of the reactivity control based on the system analysis. The system analysis is carried out to determine the intermediate events, which cause the top event. Furthermore, to calculate the probability or to quantify the failure of reactivity control and the intermediate events, the generic failure data of component, system, human error and operator error are used based on the published document [10, 11].

2. The reactivity change on the reactor operation

Based on the safety fundamental, there are ten principles to achieve the safety objective. One of those principles is to prevent and mitigate the accident and its implementation is to apply defence-in-depth concept. That concept is applied on the reactor design with the goal to fulfill the three fundamental safety functions, which are reactivity control, heat removal from reactor and fuel storage, and confinement of radioactive material.

To evaluate the fulfillment of the fundamental safety function, initiating events are postulated so that the evaluation can be done on how to mitigate all initiating events [12, 13]. Generally for the PWR design, there are five the initiating event groups to be evaluated, which are increase in heat removal from the primary system, decrease in heat removal by the secondary system, decrease in reactor coolant system flow rate, reactivity and power distribution anomalies, increase/decrease in reactor coolant inventory and radioactive release from subsystem or component. Therefore, to evaluate the first fundamental safety function on design and to obtain contribution factor to initiating events, it is important to analyze the reactivity control.

In general, the reactivity change on the PWR is caused by some events such as control rod ejection, change of boron concentration, and addition of cold water to the reactor cooling system. Those events will effect the moderation. Accordingly, the reactivity control failure is caused by the system failure that can make those three cases difficult to control [14].

The initiating event having effect significantly on the group of the reactivity control failure is caused by six cases, which are uncontrolled condition during the control rod withdrawal at low power,
uncontrolled condition during the control rod withdrawal at full power, boron dilution malfunction, misalignment during control rod withdrawal, improper positioning of fuel assembly and control rod ejection.

The uncontrolled reactivity during the control rod withdrawal is caused by malfunction of reactor control system or the failure of control rod system. The drive mechanisms of rod cluster control assembly (RCCA) are grouped into bank configurations. The purpose of grouping is to prevent automated withdrawal of other respective banks. Each bank grouping has different power supply, so that no more than two banks are withdrawn at the same time. The drive mechanisms of RCCA are the magnetic latch type and coil actuation having function to regulate speed travel. The reactor control system is initiated by the protection and safety monitoring system consisting of the source range high neutron flux reactor trip, intermediate range high neutron flux reactor trip, power range high neutron flux reactor trip, power range high neutron flux reactor trip and high nuclear flux rate reactor trip. During the full power, the protection and monitoring system consist of five events, which cause trip to the reactor. Those are 2 out of 4 channels for exceeding the overpower setpoint, 2 out of 4 channels for exceeding the over temperature ΔT setpoint, 2 out of 4 channels for exceeding the overpower ΔT setpoint, 2 out of 4 channels for exceeding the pressure at pressurizer, and 2 out of 4 channels for exceeding the water level at pressurizer.

On the normal operation, the boron dilution is manually under strict administrative controls requiring close operator surveillance. The administrative procedure is done to limit the rate and duration of the dilution. A boric acid blend system allows the operator to meet the makeup water boron concentration to the reactor cooling system during the normal charging. An inadvertent boron dilution is caused by failure of the chemical and volume control system (CVCS) due to the failure of controller, operator and mechanical.

Each RCCA has the position indicator that is checked at monitor. The failure of control rod withdrawal can be caused by malfunction of system and operator error to interpret the position or installation error after maintenance. The error of fuel assembly leading to an improper position is generated by several causes such as error in placing the fuel assembly position, error in determining the fuel pellets enrichment, and error of enrichment degree of fuel assembly. The control rod ejection accident is induced by the mechanical failure of control rod mechanism pressure housing, so that RCCA is ejected and the drive shaft is failed. The consequences of those failures contribute to the rise of rapid positive reactivity insertion, together with adversed core power distribution and finally it causes localized fuel rod damage.

3. Methodology

The principle of safety analysis using probabilistic method as the safety evaluation is to determine all initiating events considered in design, which are already identified. Also, the event probability is quantified so that the total probability can be calculated. On the evaluation, it is assumed that the smaller the probability of events at design, the higher the design safety level. The reactivity control is the first stage of the fundamental safety function. Therefore, the other fundamental safety function can function effectively if the probability of the first stage is small.

The failure probability of the reactivity control can be calculated based on determination of intermediate events as much as possible having contribution to the reactivity control. In this case, the failure of reactivity control is assumed as the top event. The cause of failure is determined by the system analysis. Furthermore, each failure reason is analyzed in detail by deductive analysis using the fault tree analysis to determine the failure cause based on basic events classified as the component failure, the operator or procedure execution error. The data of the failure or error probability used are based on generic data of the published document [10, 11]. After that, the failure probability of reactivity control is calculated as also the determination of contribution of the failure cause. The analysis diagram to be performed is shown in figure 1.
4. Results and Discussion
The Initiating event identification based on the system analysis and the failure of reactivity control using deductive analysis are shown in figure 2. The uncontrolled condition during the control rod withdrawal at low power is generally generated by mechanical and electric factor (signal to control). The mechanical factors are events which include the malfunction of control rod system, while the signal factor to move the control rod is classified as malfunction of reactor control system. The malfunction of reactor control system is caused by failure of one of the trip systems, so that the control rod can not shutdown the reactor. The trip system observation is based on neutron flux condition. For the uncontrolled condition during the control rod withdrawal at power, the logic that occurs is similar with the uncontrolled during the control rod withdrawal at low power. However, the trip to move the control rod or to shutdown the reactor is different as shown in figure 3.

In the same way, it is known that the boron dilution malfunction is caused by the system failure or the human error. The failure of the demineralized water transfer and storage system as also the CVCS are included as the system failure, while the improper dilution from the procedure and the carelessness of dilution supervision are caused by human error or operator error. The control rod
withdrawal misalignment is generated by malfunction of system and human error as operator. The error is due to the position interpretation or installation error after maintenance. Significantly, improper positioning of fuel assembly is dominated by human error especially during placement of fuel assembly position according to the core management, enrichment determination in the pellet fabrication, or determination of enrichment degree of fuel assembly. The event of the control rod ejection is dominated by the mechanical failure in the control rod mechanism pressure housing or drive shaft.

By using deductive analysis (figure 2 and 3), the calculation of reactivity control failure is carried out. The probability of intermediate events which contribute to the failure of reactivity control is showed on table 1. Based on those six intermediate events, the failure probability of reactivity control is $1.493E-03$ per year as the summed probability of intermediate events. This result is small enough if it is compared with core damage frequency (CDF). The CDF is determined by multiplying the reactivity control probability and the mitigation failure probability [15]. Therefore, the PWR design has capability to mitigate the failure of reactivity control. Also, table 1 shows that the boron dilution malfunction has largest contribution to the reactivity control failure event of 34.82%. This
event is considered as Condition II or faults of moderate frequency, so that it is not classified as an accident. The other events which are classified as Condition II are uncontrolled condition during the control rod withdrawal at low power and full power. In this analysis, the event of Condition II is 41.33%.

![Fault tree for the control rod withdrawal at full power.](image)

**Table 1.** Calculation of the failure cause probability for the reactivity control.

| No. | Intermediate event                                           | Probability, per year | Contribution | Condition Classification |
|-----|--------------------------------------------------------------|-----------------------|--------------|--------------------------|
| 1.  | Uncontrolled condition during the control rod withdrawal at low power | 2.80E-06              | 0.19%        | II                       |
| 2.  | Uncontrolled condition during the control rod withdrawal at power | 9.40E-05              | 6.32%        | II                       |
| 3.  | Boron dilution malfunction                                   | 5.18E-04              | 34.82%       | II                       |
| 4.  | Misalignment during the control rod withdrawal               | 4.43E-04              | 29.78%       | III                      |
| 5.  | Fuel assembly in an improper position                        | 4.29E-04              | 28.86%       | III                      |
| 6.  | Control rod ejection                                         | 4.36E-07              | 0.03%        | IV                       |
The second largest contribution is the misalignment during the control rod withdrawal, which is 29.78% and is classified as condition III or infrequent faults. The fuel assembly in improper position is also condition III, so that its contribution of Condition III to the failure of reactivity control is 58.46%. In this case, it needs consideration because these events are dominated by human factor.

The control rod ejection is included in Condition IV or limiting fault, which is defined as faults which are not expected but are postulated because it has the potential of the release of significant amounts of radioactive material. The result showed that the contribution of this event is very small of approximately 0.03%. The probability of this event is very small but it is included as an accident, so that it is eliminated in the design and one of the factors that is used for development of the PWR design.

Table 1 also showed that the three biggest contributions to the failure of reactivity control are affected by human error or administrative observation error. This case indicates that the human factor has influence to the failure of reactivity control, although its probability of error is still acceptable.

5. Conclusion

From the analysis, it is shown that the failure probability of reactivity control on the PWR is relatively small, which is 1.49E-03 per year and it is still within IAEA criteria. The largest contribution to the failure cause of reactivity control is given by events due to affected human factor consisting of boron dilution event, error of the control rod withdrawal, and error of fuel assembly placement. The failure probability of the reactivity control can be reduced by increasing system diversity, system redundancy and strict procedures of operation on the intermediate events.

Acknowledgment

The authors are very grateful for the financial support for this research, which is provided by DIPA 2016 of Center for Nuclear Reactor Technology and Safety.

References

[1] Kang D G, Ahn S H and Chang S H 2013 Nucl. Eng. Des. 260 165
[2] Aldemir T 2013 Ann. Nucl. Energy 52 113
[3] Lioce D, Asztalos M, Alemberti A, Barucca L, Frogheri M and Saïu 2012 Nucl. Eng. Des. 250 538
[4] Kamyab S and Nematollahi 2012 Nucl. Eng. Des. 253 32
[5] Hadad K and Kowsar Z 2016 Ann. Nucl. Energy 97 179
[6] Barati R and Setayeshi S 2014 Prog. Nucl. Energy 70 199
[7] Eisa M, Naguib M and Badawi A 2015 Ann. Nucl. Energy 81 106
[8] Parhizkari H, Aghaie M, Zolfaghari A and Minuchehr A 2016 Ann. Nucl. Energy 88 194
[9] Rabiee A and Af A 2016 Prog. Nucl. Energy 88 191
[10] Schulz T L 2007 UK AP1000 Probabilistic Risk Assessment (Westinghouse Electric Company LLC)
[11] Swain A D and Guttmann H E 1983 Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (Nuclear Regulatory Commission)
[12] Marinova B, Groudev P and Papazov V 2010 Nucl. Eng. Des. 240 880
[13] Mehboob K, Park K and Khan R 2015 Ann. Nucl. Energy 75 365
[14] Whiteman J L 2011 AP1000 European Design Control Document Rev.19 (Westinghouse Electric Company LLC) chapter 15 pp 15.4.1-37
[15] Queral J and Montero-Mayorga 2016 Ann. Nucl. Energy 91 65