Probabilistic safety Analysis for Assessing the Failure of Heat Removal Control of AP1000

D T SONY TJAHYANI, J H PURBA
Center for Nuclear Reactor Technology and Safety, BATAN
Puspiptek Complex, Building no. 80, Serpong, Tangerang Selatan 15310, Indonesia
E-mail : dtsony@batan.go.id

Abstract. The safety level of nuclear power plant can be evaluated by using the adequacy of defence in depth that is implemented in the design. The defence in depth is to fulfill requirements of the fundamental safety function, which are reactivity control, heat removal control from the reactor, and confine control of radioactive material. Those controls shall be analyzed by probabilistic safety analysis. It is important to analyze the second fundamental safety function because the first fundamental safety function has a chance to fail. The purpose of this study is to calculate of the failure probability for the second fundamental safety function that is the heat removal control. The analysis is carried out by determining top event that is the change of heat removal control. Hereinafter, the intermediate events and the basic events are selected and the failure probabilistic is calculated using failure rate of component and human error. The AP1000 is used as the object of study. The generic data is collected from IAEA and other published documents. The results show that the probability of intermediate events are 5.52E-06 to 9.11E-04 per year and the total failure probability of the heat removal control is 1.89E-03 per year. Based on the assessment, it is concluded that the failure probability of the heat removal control is small enough and still within IAEA criteria.

Keywords: Defence in depth, fundamental safety function, probabilistic safety analysis, heat removal control, AP1000

1. Introduction
The probabilistic safety analysis can be used to know the weak point of the nuclear power plant design. It can assess the safety level of the site permit to operating licenses, especially on the construction permit stage and operating licenses that are implemented in the safety analysis report. In the safety analysis, it is necessary to arrange the event sequences, which are to determine the initiating events and the mitigation systems that are the safety systems and operator actions. These actions are to deal with the initiating events, so the reactor core will not damage. In the probabilistic safety analysis, it is important to analyze the frequency or probability of initiating event and the failure of mitigation system, so that it can be known the possibility of core damage and it can be evaluated the safety level of the reactor design [1].
In the safety analysis, the initiating events were used to determine the adequacy level of the Defence in Depth (DiD) concept that has been applied in the design. To meet these requirements, the initiating events are determined based on five groups, which are to evaluate the fundamental safety functions in the design that are to control the reactivity or the operating, to remove heat from the reactor and to confine radioactive materials or retaining radiation. The important parameter that is considered is to remove heat from the reactor in all operating conditions after the reactor can be shutdown. In the light water reactor (LWR), to control heat removal from the reactor core including heat transfer to ultimate heat sink (UHS) is an important process because of the decay heat. This controlling is to prevent the core damage or the severe accident.

Currently the pressurized water reactor (PWR) type under construction is generation III+ based on active systems (US-APWR and EPR), as well as passive system (Advanced Passive Pressurized Water Reactor, AP1000). Nevertheless, after the Fukushima accident and under the IAEA guidance, the passive system technology gained more attention [2]. The AP1000 is a PWR type that implemented totally the passive principle to the passive core cooling systems (PXS) [3]. The PXS consist of the core makeup tank (CMT), the passive residual heat removal (PRHR), and the automatic depressurization system (ADS). The implementation of passive systems on PWR is based on difference in density and position of the cooling water level. It will cause a natural driving forces, buoyancy and circulation flow. This principle is particularly useful for covering in the event of the station blackout (SBO), so that the system can naturally function toward a safe state, without requiring the active system to function.

Research that is related to the AP1000 based on passive systems in the heat removal process is mostly carried out, such as the study of passive containment cooling system capability in LOCA (Loss of Coolant Accident) condition [4], analysis of passive core cooling system performance to mitigate DVILB (Direct Vessel Injection Line Break) using RELAP5 / SCDAP / Mod 3.4 [5], analysis of IRWST (In-containment Refueling Water Storage Tank) capabilities to mitigate the initiating event in long term conditions [6], assessment of ADS (Automatic Depressurization System) capabilities to control pressure based on availability other systems [7], the study of the PRHR (Passive Residual Heat Removal) performance [8], and the reliability study of the AP1000 passive safety system [9]. The heat removal control is second stage after reactivity control to prevent core damage. Based on the probability analysis, the reactivity control has a chance to fail [10]. Therefore, to evaluate the safety characteristic of AP1000, the failure analysis of heat removal shall be carried out. The result of analysis can be used to modify the cooling system on the design of AP1000. Furthermore, the adequacy level of fundamental safety function can be evaluated.

The fundamental safety functions consist of reactivity control, heat removal control and confinement of radioactive materials. Until now, the calculation of the failure probability for the heat removal control is not yet carried out. So, the purpose of this study is to calculate of the failure probability for the second fundamental safety function that is heat removal control. This research objective can be achieved through the PSA by the Fault Tree Analysis. The AP1000 that is based on passive system is used as the object of study. The analysis is done by deductive analysis that is the fault tree analysis of the heat removal failure. The top event is selected based on the system analysis. Furthermore, The component failure, system failure and human error based on published data [11,12] are used to calculate the top event probability.

2. The heat removal from the reactor core of AP1000

In relation with the heat removal control, there are five group of initiating events, 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, increase in reactor coolant inventory and
decrease in reactor coolant inventory. In general, the change of heat transfer is caused the system failure that affect to heat transfer process and change of coolant temperature. Therefore, it will influence moderation process and reactivity.

The increase in heat removal from the primary system is caused by malfunctions for feedwater system, excessively increasing for steam flow in secondary system, inadvertent opening for safety valve or relief valve in steam generator, failure of steam system piping, and inadvertent operation for heat exchanger of PRHR. There are eight intermediate events that caused the decrease in heat removal by the secondary system. Those events are malfunction for steam pressure regulator, loss of external electrical load, turbine trip, inadvertent closure of MSIV (main steam isolation valve), loss of condenser vacuum and other events affecting in turbine trip, loss of AC power to the auxiliaries system, loss of normal feedwater flow and breaking of feedwater system pipe.

The decrease in reactor coolant system flow rate is caused by partial loss of forced reactor coolant flow, full loss of forced reactor coolant flow, shaft seizure for RCP (reactor coolant pump) and shaft break for RCP. The increase in the reactor coolant inventory is caused by inadvertent operation for CMT on the full power and malfunction for CVCS. Furthermore, the intermediate event of decrease in the reactor coolant inventory is caused by inadvertent opening of safety valve or inadvertent operation of ADS, break in instrument line, steam generator tube failure and LOCA due to postulated piping breaks.

The decrease in reactor coolant system flow rate is caused by the partial loss of forced reactor coolant flow, the full loss of forced reactor coolant flow, the shaft seizure for RCP and the shaft break for RCP. The increase in reactor coolant inventory is caused by the inadvertent operation for CMT on the full power and the malfunction for CVCS. The decrease in reactor coolant inventory is caused by the inadvertent opening of safety valve/operation ADS, the break in instrument line, the steam generator tube failure and the rupture of piping.

Based on the frequency of occurrence and potential of radiological consequences on the public and environment, the initiating events are classified into 4 (four) conditions, which are normal operation and operational transient, faults of moderate frequency, infrequent faults and limiting faults [13]. The classification of initiating events for the heat removal is shown in Table 1.

| No. | Initiating Event                                                      | Condition Classification |
|-----|-----------------------------------------------------------------------|--------------------------|
| 1.  | Increase in Heat Removal from the Primary System                       | II, III, IV              |
| 2.  | Decrease in Heat Removal by the Secondary System                       | II, IV                   |
| 3.  | Decrease in Reactor Coolant System Flow Rate                           | II, III, IV              |
| 4.  | Increase in Reactor Coolant Inventory                                  | II                       |
| 5.  | Decrease in Reactor Coolant Inventory                                  | II, III                  |

Table 1. Classification of initiating events for heat removal failure [13].
3. Methodology
The analysis is done by using fault tree analysis (FTA). The top event is determined by using assumption the events that influence against the change of heat transfer process and coolant temperature. Furthermore, the intermediate events is selected based on top event. The failure probability is calculated by using basic events, which are component failure and human action error. The data of failure rate and error rate is selected by using generic data of the published document [11,12]. Hereinafter, the contributions failure of top event is determined based on the probability of intermediate events. The flowchart of analysis is presented in Figure 1.

![Flowchart of analysis.](image)

4. Results and Discussion
Based on the top event of heat removal change and by using the deductive analysis, there are five intermediate events that are increase in heat removal from the primary, decrease in heat removal by the secondary system, decrease in reactor coolant system flow rate and decrease/increase in
reactor coolant inventory, as shown in Figure 2. Hereinafter, the intermediate event of increase in heat removal from the primary system is caused several events, which are malfunction of feedwater system, increasing for steam flow, inadvertent opening for steam flow, failure of steam system piping and inadvertent operation for heat exchanger of PRHR. Malfunction of feedwater systems are caused decrease in feedwater temperature or increase in feedwater flow as shown in Figure 3. The reduction in feedwater temperature will decrease the reactor coolant temperature and the power reactor will increase. The change of feedwater temperature is caused by out of service for low pressure heater train or high pressure heater train. The increase in feedwater flow will cause decreasing reactor coolant temperature as a result the power reactor will increase. The change of this event is caused malfunction of feedwater control system or operator error. The increasing for steam flow in secondary system also induce the increase in heat removal from the primary system. This event is due to operator error, malfunction steam dump control and malfunction of turbine speed control as shown in Figure 3. Result of the increasing for steam flow effect to the power mismatch between the reactor core power and the steam generator load.

![Fault tree for the failure of heat removal from core.](image)

The event of inadvertent opening for safety valve or relief valve is caused in advertent opening for steam dump, safety valve or relief valve. This event influences the energy removal from the reactor coolant system that causes a reduction of coolant temperature and pressure, so that the negative moderator temperature is occurred. This phenomenon will generate the positive insertion reactivity. The event of the failure of steam system piping is caused steam line leakage or steam line rupture. This event generates the positive reactivity as the event of inadvertent opening for valve. The event of inadvertent operation for heat exchanger of PRHR causes injection of cold water into the reactor coolant system. This phenomenon produces the positive reactivity. This event is due to operator error, inadvertent actuation for heat exchanger of PRHR or malfunction of isolation valve. The inadvertent actuation for heat exchanger of PRHR is caused by operator error or a false actuation signal.
The intermediate event of decrease in heat removal by the secondary system is caused by malfunction for steam pressure regulator, loss of external electrical load, turbine trip, inadvertent closure of MSIV, loss of condenser vacuum, loss of AC power to the auxiliaries system, loss of normal feedwater flow or breaking of feedwater system pipe. Furthermore, the intermediate event of decrease in reactor coolant system flow rate is due to partial loss of forced reactor coolant flow, full loss of forced reactor coolant flow, shaft seizure for RCP or shaft break for RCP.

The intermediate event of increase in the reactor coolant inventory is caused by inadvertent operation for CMT or malfunction for CVCS, while the intermediate event of decrease in the reactor coolant inventory occurred because of inadvertent opening for safety valve, break in instrument line, steam generator tube rupture or piping breaks.
Figure 3. Fault tree for the increase in heat removal from the primary system.

By using deductive analysis, the failure probability of heat removal is carried out by the failure rate or demand probability, some data is presented in Table 2. The probability of intermediate event is determined as presented in Figure 4. The probability of intermediate events are 5.52E-06 to 9.11E-04 per year and the failure probability of heat removal is 1.89E-03 per year, which are the sum of the failure probability of five intermediate events. The probability of intermediate event of increase in heat removal is the largest if it is compared with the other intermediate events. The event that is largest contribution to this intermediate event is the failure of steam system piping, which is mechanical failure. The probability for intermediate event of decrease in reactor coolant inventory that may arise LOCA is small enough. The probability for intermediate event of increase in reactor coolant inventory, which can affect to moderation process is small too. This is because CMT and CVCS have high reliability.

Table 2. Failure rate/demand probability for basic event/system [11, 12]

| No. | Basic event                              | Failure rate/probability, hour⁻¹/demand⁻¹ |
|-----|------------------------------------------|------------------------------------------|
| 1   | Failure of Control System                | 6.60E-04                                 |
| 2   | Operator Error to Operate the system or component | 3.30E-02                                 |
| 3   | Operator Error to Response               | 1.60E-03                                 |
| 4   | Operator no response to incident         | 1.84E-03                                 |
| 5   | Failure of control adjustment            | 8.00E-05                                 |
| 6   | Malfunction of Feed water Control System | 9.15E-07                                 |
| 7   | Malfunction of Steam Dump Control        | 3.00E-06                                 |
| 8   | Inadvertent Opening for Steam Dump       | 1.00E-05                                 |
| 9   | Inadvertent Opening for Relief Valve     | 7.20E-07                                 |
| 10  | Inadvertent Opening for Safety Valve     | 7.20E-07                                 |
| 11  | Steam Line Leakage                       | 7.45E-04                                 |
|   | Event Description                                    | Probability     |
|---|------------------------------------------------------|-----------------|
| 12 | Steam Line Rupture                                  | 2.40E-06        |
| 13 | Inadvertent Actuation for Heat Exchanger of PRHR    | 5.10E-05        |
| 14 | Malfunction of Isolation Valve                      | 9.15E-07        |
| 15 | Malfunction of Electrical Control System            | 4.80E-06        |
| 16 | Mechanical Failure                                  | 2.70E-06        |
| 17 | Disturbance of Electrical System                    | 6.00E-05        |
| 18 | Pump Failure                                        | 7.10E-06        |
| 19 | Loss of Offsite Grid                                | 6.00E-05        |
| 20 | Steam Generator Tube Failure                         | 1.20E-09        |

Figure 4. Calculation result of the failure cause probability for heat removal control.
The contribution of the failure cause for heat removal is presented in Figure 5. The first largest contribution is about 48.17% and is classified as condition II and III especially steam line rupture is classified as condition IV. The second largest contribution that is decrease in heat removal by the secondary is 42.05% and is classified as condition II, excepted the event for breaking of feedwater system piping is classified as condition IV. The third largest contribution is 5.04%, which is decrease in reactor coolant system flow and it is classified as condition II and III, while shaft seizure and shaft break for RCP is classified as condition IV.

Based on this analysis, the failure probability of heat removal is small enough. Therefore, the second fundamental safety function on the PWR, which are heat removal from the reactors and fuel storage has high capability. Hereinafter, The PWR design can mitigate all condition for operation modus.

5. Conclusion
From the analysis, it is shown that the failure probability of heat removal control of AP1000 is 1.89E-03 per year, which is small enough and still within IAEA criteria. There are five contributors to the failure of the heat removal control. The largest contributor is the increase in heat removal from the primary system whose failure probability is 9.11E-04 per year (48.17%).

Acknowledgment
The authors are very grateful for the financial support for this research, which is provided by DIPA 2017 of Center for Nuclear Reactor Technology and Safety.

References
[1] Sony Tjahyani D T and Purba J H 2014 Tri Dasa Mega 16 (3) 134-148
[2] Winter J 2008 AP1000: Passive System (Westinghouse Electric Company LLC)
[3] Schultz T L 2006 Nucl. Eng. Des. 236 1547-1557
[4] Hung Z Y, Ferng Y M, Hsu W S, Pei B S and Chen Y S 2015 Ann. Nucl. Energy 85 717-724
[5] Ekariansyah A S and Widodo S 2016 Atom Indonesia 42 79-88
[6] Quan L Y, Jian C H, Li L D, Yan S, Shen Y Z, Kai Y and Fang F 2016 Ann. Nucl. Energy 88
218-236

[7] Hashim M, Hidekazu Y, Takeshi M and Ming Y 2014 *Nucl. Eng. Des.* 278 209-221
[8] Zou J, Li Q, Tong L L and Chao X W 2014 *Prog. Nucl. Energy* 70 159-166
[9] Purba J H and Sony Tjahyani D T 2014 *Atom Indonesia* 40 49-56
[10] Sony Tjahyani D T, Deswandri and Sunaryo G R 2018 *J. Phys.: conf. Ser.* 962 012046
[11] Schulz T L 2007 *UK AP1000 Probabilistic Risk Assessment* (Westinghouse Electric Company LLC)
[12] Swain A D and Guttmann H E 1983 *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications* (Nuclear Regulatory Commission)
[13] Whiteman J L 2011 *AP1000 European Design Control Document Rev.19* (Westinghouse Electric Company LLC) chapter 15 pp 15.1-3, 15.5-6