Probabilistic Safety Analysis for Loss of Offsite Power Accident in Dual-units Nuclear Power Plant

Wanxin Feng1,2, Zhixin Xu1, Mingzhu Zhang2, and Yu Yu2 *

1State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, China Nuclear Engineering Co., Ltd, Shenzhen of Guangdong Prov.518172, China
2School of Nuclear Science and Engineering, Beijing Key Laboratory of Passive Nuclear Safety Technology, North China Electric Power University, Beijing 102206, China

Abstract. In order to explore the risk assessment method of the multi-unit nuclear power plant site, this paper selects the dual-unit plant nuclear site to analyze lose off-site power accident. By combining and improving the single-unit ET/FT model, to establish the dual-unit ET/FT model. From the analysis of the accident sequence, it can be concluded that the common cause failure of equipment is the main challenge faced by the dual-units. Especially the RPC sub-channel in the reactor protection system and the failure of emergency diesel engine circuit breaker. As can be seen from the high proportion of core CD occurring simultaneously in both units, it has a great significance to study the risk of multi-units sites.

1 Introduction

Traditional nuclear power plant Probabilistic Safety Assessments (PSA) are conducted for the single reactor, but the reality is that the vast majority of nuclear power plants currently in operation or under construction are multi-unit sites. Since the Fukushima disaster, the international community has paid great attention to the risk assessment of multi-unit sites[1]. There are multiple reactors in the same site, and several of these reactors have accidents at the same time. Multi-units sites risk assessment will contribute to the comprehensive safety improvement of nuclear power plants[2].

PSA a system engineering method developed after the 1970s, adopts FT/ET (fault tree analysis, event tree analysis) and probabilistic risk analysis method to comprehensively analyse various possible accidents of complex systems, and comprehensively consider the probability of the accidents and its consequences. Probabilistic safety analysis is a standard tool for nuclear power plant safety assessment[3]. We can improve the single-unit probabilistic safety analysis method to analyse multi-unit sites.

In multi-unit PSA model, the key points that need to be paid great attention include, common structures, systems, and components (SSCs), common cause failure(CCF) among different units and so on. Loss of Offsite Power (LOOP) accident is one of the most important initiating event in nuclear power plants. This paper establishes a dual-unit event sequence to calculate and analyses the consequences.

2 Method

2.1 Procedure for estimating site CDF

The site CDF due to mult-unit was estimated using the following steps[4]:

1) Estimation of the multi-unit initiating event frequency on a per site-year basis.
2) Construction of a single-top fault tree logic for the site CDF model.
3) Development of each individual unit model based on the base single-unit model, and integration of each unit model into the top logic.
4) Modification of the single-top fault tree considering inter-unit dependencies.
5) Quantification of the accident sequence frequencies.

Procedure for estimating site CDF due to each MUI

![Fig. 1. Modelling of double units](image)
As shown in Figure 1, the single unit PSA model in the form of a single top fault tree needs to be modified. Then they are coupled into a site CDF model. Fault tree logics unrelated to the initiator being analysed were deleted. In the LOOP accidents, it is important to consider: (1) Common-cause Initiating events, (2) SSCs shared between two units (3) inter-unit CCFs.

2.2 Establishment of the loss of offsite power (LOOP) accident model for two units

The research object of this paper is a million kW pressurized water reactor (PWR) nuclear power plant with two units. Based on the existing single-unit PSA model, considering the interdependence between the two units, the dual-unit ET/FT model is formed by coupling to conduct static analysis.

LOOP accident refers to the loss of both the main and auxiliary off-site power grids. Considering the loss of offsite power, if the emergency diesel generator sets fail, the unit will face more serious station blackout accident. In order to make a clearer analysis, the event tree of the station blackout is also established for analysis.

The event process and system response are as follows:

1. **Loss of offsite power**: The loss of offsite power caused the main pump to shut down, and a low signal was issued due to the low speed of the main pump. In addition, the power supply of the control rod drive mechanism was lost, and the control rod fell due to gravity. All of these led to the emergency shutdown of the reactor.

2. **Emergency shutdown**: If the emergency shutdown fails, it will cause the expected transient state of failure to shutdown. After the emergency shutdown, if the emergency diesel engine fails to be put into operation, the accident develops into station blackout. After the loss of off-site power supply, if the emergency diesel engine is available, the unit will re-establish the secondary side cooling of the core, and the steam pressure in the primary circuit will rise, which may cause the pressurizer safety valve to open.

3. **Loop accident**: If the safety valve cannot fall will cause small-break loss-of-coolant accident. If the secondary side cooling fails, the safety injection system can be started and the pressurizer safety valve can be opened to perform a "charge and discharge" operation to cool the core.

4. **Station blackout**: If both fail, the core residual heat cannot be discharged. After the station blackout, pneumatic pump of the auxiliary feedwater system supplied water to cool the secondary side, which became the only means of core cooling.

If the auxiliary water supply system fails, the core residual heat will not be able to be taken out. At this time, it can only rely on the restoration of AC power, or the additional diesel generator sets to provide power, so that the auxiliary feedwater electric pump can provide water to cool the core. In addition, the safety injection system can be used to implement "charge and discharging" operation, it is also necessary to open the pressurizer release valve and put in the containment spray system.

3 Results and discussion

After the LOOP accident occurs, the safety systems in the nuclear power plant are activated in turn to provide...
corresponding safety functions to mitigate the accident. Redundant design is often used in nuclear power plants to ensure that have sufficient safety margins. And common cause failures (CCF) often occur among same type components. CCF is considered to be the main cause of system failure and core damage. In this article, multiple Greek Letter and MGL model are used to establish CCF event group. The data of demand failure probability, operational failure probability and common cause failure probability of related equipment are all from the reports provided by the cooperative unit.

Table 1 CDF calculation result

|    | UNIT-A   | UNIT-B   | UNIT-2   | MUI     |
|----|----------|----------|----------|---------|
| CDF| 3.94E-07 | 3.94E-07 | 5.34E-07 | 2.54E-07|

The table 1 summarizes the core damage frequency numerical value of different units in the site. The CDF in case of LOOP for A and B are listed respectively, and the unit-2 represents the CDF calculated through the model of at least one of the two units with core damage. According to the probability formula:

\[ P(A \cap B) = P(A) + P(B) - P(A \cup B), \]

The total CDF of two reactors damaged at the same time is 2.54e-07. This data accounts for 47.6% of the core damage frequency of any LOOP accident. Which means that for dual-units site, once the LOOP occurs, there’s a 47.6% possibility that both cores will be damaged at the same time.

Table 2 Core damage minimum cut set table

| Accident sequence | Proportion | CDF     | Basic Event                  |
|-------------------|------------|---------|------------------------------|
| E1                | 36.78%     | 1.97E-07| GEVTPN-IE-LGJ-JA-RC          |
|                   |            |         | I&C-RPC-A-                   |
|                   |            |         | LHA-                         |
| E2                | 8.11%      | 2.20E-08| GEVTPN-IE-LGJ-ALL           |
|                   |            |         | LHB002JG2RC-LLS001APL-FR    |
| E3                | 7.62%      | 2.05E-08| GEVTPN-IE-LGJ-ALL           |
|                   |            |         | LHB001JG2RO-LLS001APL-FR    |
| E4                | 4.11%      | 2.90E-08| GEV001TSF-IE-JA-RC         |
|                   |            |         | I&C-RPC-A-                   |
|                   |            |         | CPU-UF-ALL                  |
| E5                | 3.04%      | 1.63E-08| MAIN-CON-IE-JA-RC           |
|                   |            |         | I&C-RPC-A-                   |
|                   |            |         | CPU-UF-ALL                  |

Through the fault tree analysis of the systems involved in the event tree, the occurrence probability of the top event of the fault tree can be obtained. By connecting the failure probability of the top event quantified by the fault tree with the event tree, the frequency of core damage caused by the LOOP accident of the dual-reactor nuclear power plant will be obtained. The great final failure frequencies are owned by the following five sequences:

E1, E4 and E5 are all caused by the loss of the main external power grid, and the failure of off-site auxiliary power source leads to the loss of off-site power. The common cause failure of the CPU cabinet in the reactor protection system resulted in the failure of various mitigation measures, and the core CD. Among them, E1 refers to the operation failure of the main transformer, E4 refers to the operation failure of the common transformer, and E5 refers to the operation failure of the main external network wiring.

The function of the reactor protection system is to prevent the reactor from running beyond the safety limit. After the relevant parameters exceed the safety limit, the shutdown protection and specially set safety facilities can be timely operated to make the unit reach a controllable state as soon as possible. The four channels of the RPC subsystem in the reactor protection system measure the protection parameters, and when the appropriate logical combination is met, the signal is triggered, the shutdown circuit breaker is invoked, and other specially designed safety device drives are used. The common cause failure of data channels leads to serious consequences.

E2 and E3 are both the loss of off-site power, the common cause failure of closing/opening the circuit breaker refuse to the failure of the emergency diesel, station black-out accident occurred, and the operation failure of LLSAP caused the LLS (Hydraulic Test Pump Diesel Generator Set System) system to be unavailable and unable to provide seal water to the main pump. After a 15t/h break LOCA occurred in the shaft seal, the
auxiliary feedwater system fails, the common cause failure of additional diesel engine because of the circuit breaker, and other available systems cannot be put into operation to alleviate the accident, finally, the core CD.

4 CONCLUSIONS

In this paper, the dual-reactor PSA model is used to carry out probabilistic safety analysis on the LOOP accident of the double-units plant site. All possible response paths of the plant after the accident are obtained by the ET/FT method. The top five accident sequences are sorted out, as well as the core damage frequency analysis of the entire plant site. From the analysis of the accident sequence, it can be concluded that the common cause failure of equipment is the main challenge faced by the double-units. Especially the RPC sub-channel in the reactor protection system and the failure of emergency diesel engine circuit breaker. It can be seen from the results that the ratio of core CD of two reactors at the same time caused by the LOOP accident is 47.6%. Thus it can be seen that the LOOP accidents is of great significance in the safety analysis and evaluation of multi-reactor.

Through the analysis and study of the dual-reactor model, the weak links in LOOP events of nuclear power plants can be found, so as to improve the reliability of related equipment. In addition, the dynamic method can be considered for further analysis due to the loss of time redundancy in the response of emergency diesel engines in off-site power accidents.

Acknowledgments

This work was supported by State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment.

References

1. NRC. Reactor safety study: An assessment of accident risks in U.S. commercial nuclear power plants, WASH-1400 (NUREG 75/014) [R]. Washington D.C., US:NRC, 1975
2. NRC. Safety goals for the operations of nuclear power plants: Policy statement, 51FR30028[R]. Washington D.C., US: NRC, 1986.
3. Safety Reports Series No.96, Technical Approach to Probabilistic Safety Assessment for Multiple Reactor Units[R]. VIENNA: INTERNATIONAL ATOMIC ENERGY AGENCY,2019.
4. Dong-San Kim, Sang Hoon Han, Jin Hee Park, et al. Multi-unit Level 1 probabilistic safety assessment: Approaches and their application to a six-unit nuclear power plant site. Nuclear Engineering and Technology, Vol.50, pp1217-1233, 2018.