Transition of the mission success probability with the progression of nuclear power plant accident

MATSUOKA Takeshi [1, 2]

1. College of Nuclear Science and Technology, Harbin Engineering University, Harbin, 150001, China
2. Center for Fundamental Education, Utsunomiya University, Utsunomiya City, Japan (mats@cc.utsunomiya-u.ac.jp)

Abstract: In case of a nuclear power plant accident, the plant configuration drastically changes and required missions also change. The GO-FLOW is applied to estimate mission success probabilities of nuclear power plant system under severe accident conditions. A hypothetical sequence of accident conditions has been settled based on the Fukushima Daiichi accident. The following conditions are considered in the analysis. Loop structures in nuclear power plant system. Many components are placed in high stressed condition in an accident, and common cause failures have to be considered in reliability analyses. For the prevention of accident, “ad hoc” and “flexible” actions are required. It is pointed out the necessity of the estimation of human performance in reliability analysis. The results are expressed in graphical style which will correspond to a display window of risk monitor system, which visualizes risk state intuitively. The analysis procedure presented here indicates that mission success probabilities with the progression of accident are easily obtained by using the GO-FLOW methodology.
Keyword: nuclear safety; reliability analysis; availability; loop structure; common cause failure; GO-FLOW

1 Introduction

In case of a nuclear power plant accident, especially in severe accident, the plant configuration drastically changes and required missions for safety operation of plant or prevention of escalation of accident also change [1]. The plant states dynamically change with the progression of accident. In this paper, the GO-FLOW [2] is applied to estimate mission success probabilities of nuclear power plant system under severe accident conditions.

A hypothetical sequence of accident conditions has been settled based on the Fukushima Daiichi accident, from a normal operation, loss of offsite power, station blackout, core cooling by emergency core cooling systems and to core cooling by sea water with fire protection pump. Success probabilities of system operation, or prevention of core damage are quantitatively evaluated by the GO-FLOW methodology.

The results are expressed in graphical style which will correspond to a display window of risk monitor system [3], which visualizes risk state intuitively as "dynamic risk monitor". The analysis procedure presented here indicates that mission success probabilities with the progression of accident are easily obtained by using the GO-FLOW methodology.

2 Systems analyzed under accident conditions

Figure 1 shows a general layout of BWR system. Only essential parts are expressed. The system has been already taken up [1] for the evaluation of the dynamic behavior.

It is seen there are five essential loop structures, main steam and feed water loop, electric power supply, component cooling water supply, steam extraction, and lubricating oil system. The brief explanation of how to solve loop structured system in reliability analysis is given in chapter 5. The details of analysis procedure of loop structure are explained in reference [4].

Under the accident condition "station blackout", the mission of the plant is "core cooling". The reactor core isolation cooling system (RCIC) and high pressure core injection system (HPCI) are successively used for this purpose. The layout of the systems are shown in Figs 2 and 3.

From Figs. 2 and 3, we can see there are commonly used components for both systems. So, the successive operation of two systems becomes a phased mission problem. Also, these two systems have common components with the power generation system of BWR nuclear power plant (Fig.1). Common components are "main steam line", "pressure vessel (reactor vessel)" and "feed water line", but failure rates of these components are very small. Therefore, it is not necessary to consider phased mission condition for the operation change from "power generation" to "core cooling".

After the failure of two systems: RCIC and HPCI, fire engine is brought and fire protection pump is used for injection of pure water or sea water. The system layout is shown in Fig. 4, which is actually taken at the Fukushima Daiichi accident [5].

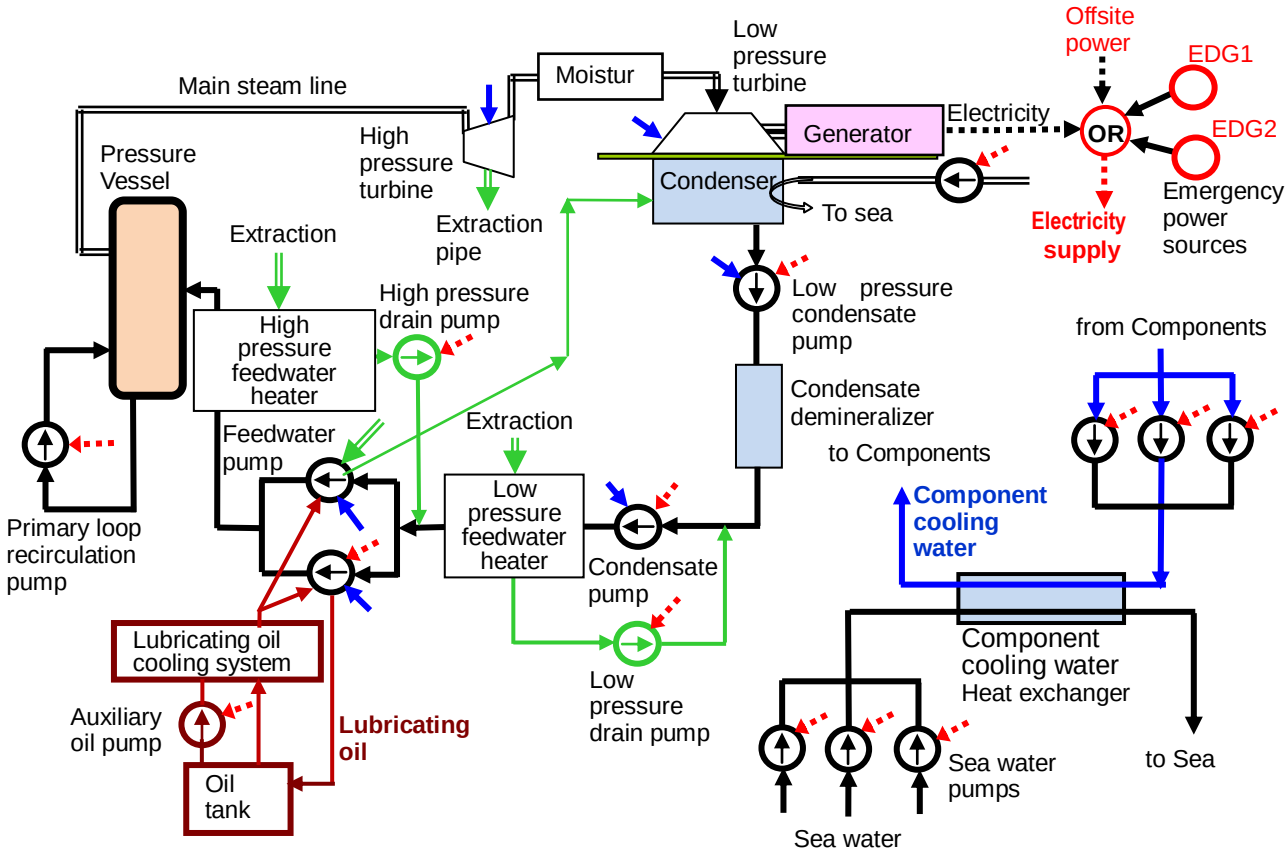

Fig.1 General layout of BWR nuclear power plant.

3 A hypothetical sequence of accident

Following accident sequence is assumed.

Initially, nuclear power plant is in normal operating states. At a certain point, offsite power is lost, but power generation is maintained with the start of emergency diesel generators. Next, one of two emergency generators fails, still the function of power generation is maintained. Finally, the second generator also fails. Even in this case, the plant is designed to be possible to continue its operation with loop structures as shown in Fig.1. In the actual operating procedure of nuclear power plants, the operation is immediately stopped if offsite power is lost.

In the next stage, reactor is shut down. There is no AC power source, that is, plant is placed in "station blackout" condition. The mission of the plant has changed from "power generation" to "core cooling". The reactor core isolation cooling system (RCIC) and high pressure core injection system (HPCI) are successively used for core cooling. It indicates that small amount of DC power is available for the operation of motor operated valves.

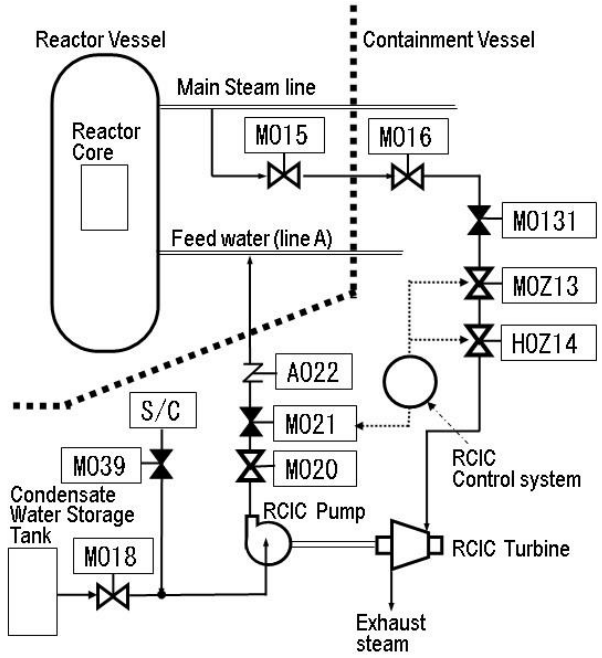

Fig. 2 Reactor core isolation cooling system (RCIC) of Fukushima-Daiichi units 2&3.

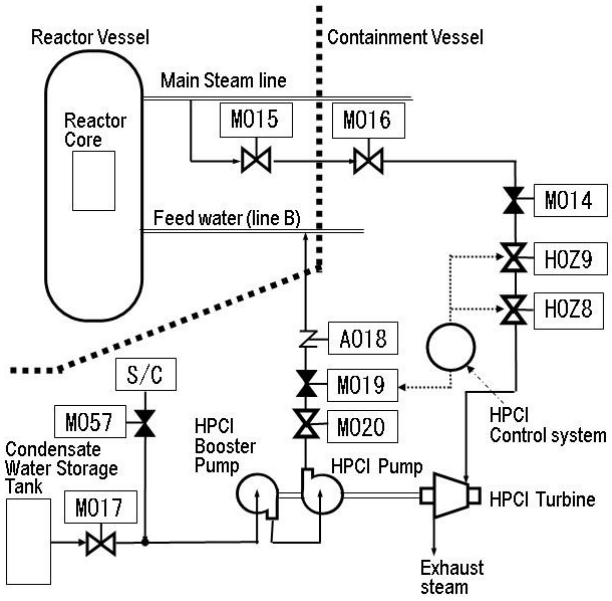

Fig. 3 High pressure coolant injection system (HPCI) of Fukushima-Daiichi units 1,2,3.

HPCI is designed to inject large amount of coolant, so the reactor pressure rapidly decreases after the start of HPCI. Power of the turbine driven pump(HPCI pump) also rapidly decrease and HPCI cannot continue the injection of coolant for long time duration. In the accident of Fukushima Daiichi unit 3, pressure of the pressure vessel decreased under 2MPa about 5hours after the start of HPCI.

After the failure of both systems (RCIC and HPCI), a fire protection pump is connected to the primary cooling system, and the core is cooled by the water from pure water tank in the plant site. The fire pump is driven by diesel generator brought by a car. After the pure water tank is exhausted, the core is cooled by sea water, and waits to recover external power supply.

4 Failure data

Failure rates of components are assigned as follows based on the data shown in the standard for procedures of Level 1 PSA[6] and component reliability data collected by IAEA[7].

Motor/Air operated valve	
failure of open/close action	3.6×10^{-3}/D
failure during usage	2.0×10^{-7}/hour
failure during standby	2.0×10^{-8}/hour
Pump	
fails to start	2.7×10^{-2}/D
failure during operation	1.0×10^{-4}/hour
Emergency diesel generator	
fails to start	1.0×10^{-2}/D
failure during operation	3.0×10^{-3}/hour
Fire engine	
Fails to connect	1.4×10^{-2}/D
Fire pump	
fails to start	2.7×10^{-2}/D
failure during operation	1.0×10^{-4}/hour
Turbine	
fails to start	2.7×10^{-2}/D
failure during operation	1.0×10^{-4}/hour
Condensate water storage tank	
failure during operation	2.8×10^{-8}/hour

5 Procedure for solving a system with loop structures

For a system which has logical loop structure(s), the Boolean relations have to be described with unknown variable(s) "x" as shown in equation (1).

$$x = f(\alpha_1,\cdots,\alpha_n)x + g(\alpha_1,\cdots,\alpha_n)\ . \qquad (1)$$

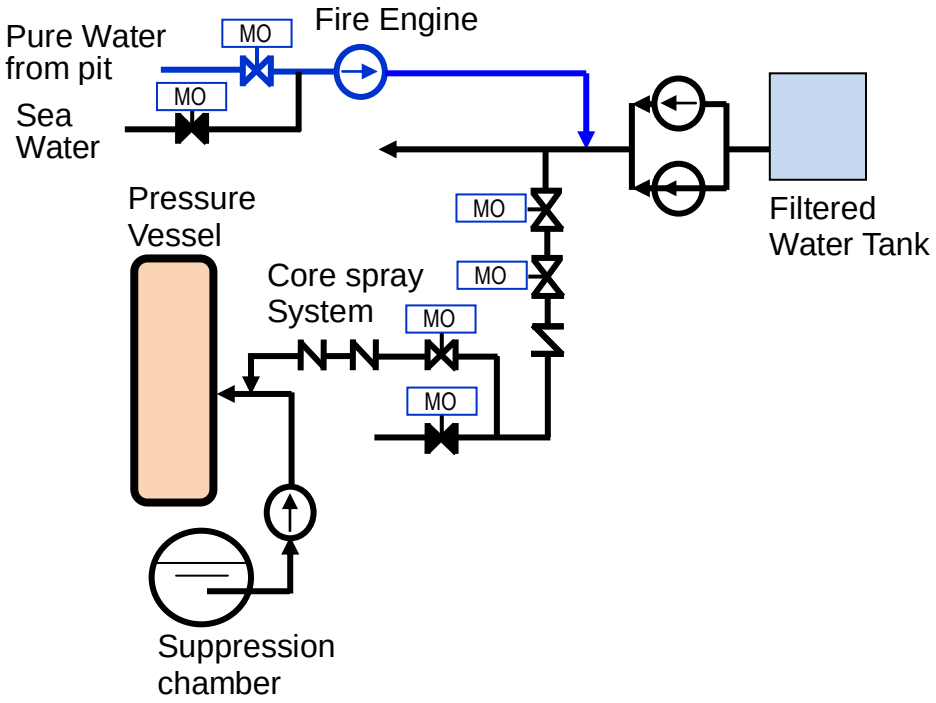

Fig.4 Water injection by fire engine.

If we try to solve the above equation, we encounter infinite circulation of the unknown variable(s). Logical loop was not generally solved in terms of the arithmetic operators of Boolean algebra. The solution of equation (1) becomes:

$$x = mf\left(\alpha_1,\cdot\cdot,\alpha_n\right) + g\left(\alpha_1,\cdot\cdot,\alpha_n\right). \qquad (2)$$

The unknown element *"x"* can be expressed by "α_t " and "*m*" without *"x"*. Where "*m*" is an indefinite arbitrary element. Basically, a loop structure can be solved [8].

It is necessary to determine *"m"* in order to obtain a solution which correctly represents the reliability or availability of an actual engineering system. "Takeover" phenomenon has essential role to establish loop operating state. It has been shown that arbitrary Boolean element "*m"* must be "unity" or "a universal set" under the condition that Boolean elements represent operating states of components[8].

6 Analysis conditions and modeling

6.1 Success probability of BWR plant operation -Loop structure and Common cause failure-

In Fig. 1, red arrows indicate electric power supply. If components have red arrow, they require electricity for their operation. Blue arrows indicate cooling water, and components require to be cooled by water, when they have blue arrow. Green lines indicate extraction steam lines. Reactor feed water pump needs lubricating oil for its continuous operation. These loop structures are solved by using the method explained in chapter 5, and the Boolean relations are obtained, which represent the operational states of BWR system. The reliability of BWR system is calculated by the GO-FLOW methodology. The GO-FLOW chart is constructed as shown in Figs. 5, which contains the logic of loop structures.

In this analysis, common cause failures are considered. Assume all the motor operated valves (MOVs) are suffered common causes and simultaneous failures will happen with certain rate. Many methods are proposed for the analysis of common cause failures[9]. The β-factor method is used for the estimation of the contribution from common cause failure of MOVs in the GO-FLOW analysis [10]. The GO-FLOW chart needs not explicitly express the common cause failure relations[11]. In the analysis, common cause failures are considered for MOV operating failures (Group1; No.46,48, β=0.3, Group2; No.20,22, β=0.3, Group3; No.31,39,40,

β=0.3, Group4; No.35,37,38, β=0.3). Where No.46 means operator number 46 in Fig.5.

6.2 Core cooling by RCIC and HPCI

Under the accident condition "station blackout", the mission of the plant is "core cooling". The reactor core isolation cooling system (RCIC) and high pressure core injection system (HPCI) are successively used for this purpose. If RCIC fails, the HPCI is immediately started its operation for the core cooling. But, HPCI cannot continue the injection of coolant for long time duration. It is assumed that the pressure of the pressure vessel decreased under 2MPa about 5hours after the start of HPCI.

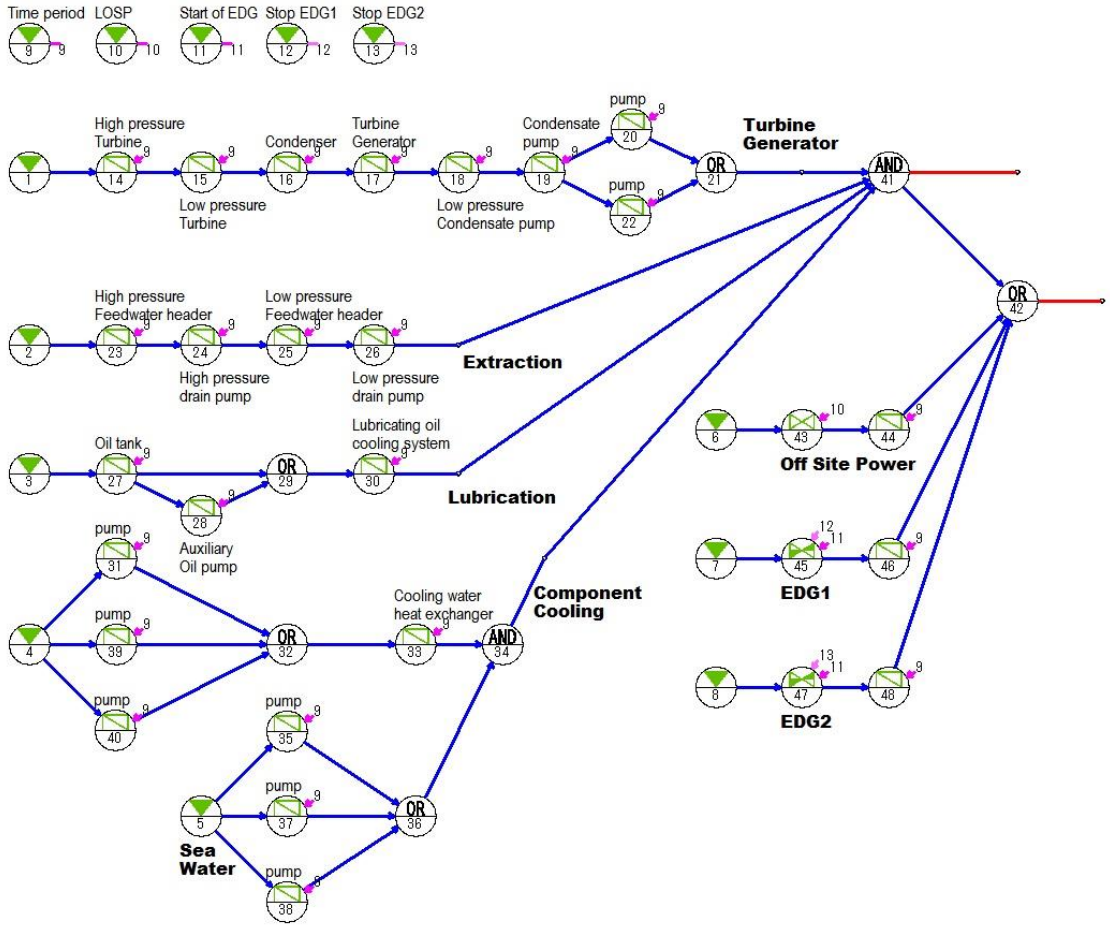

Fig.5 GO-FLOW chart for general layout of BWR nuclear power plant.

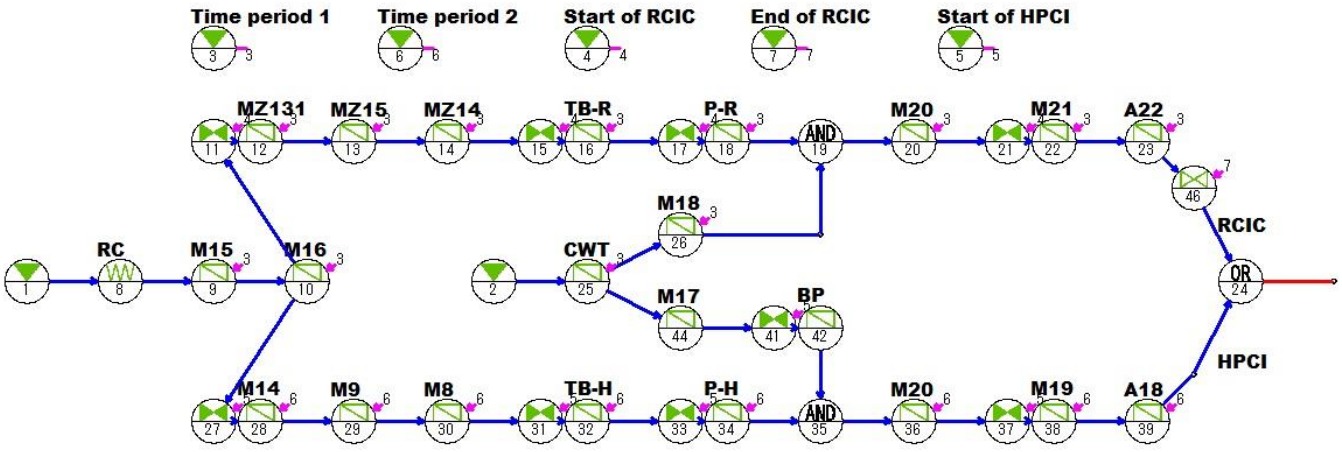

Fig. 6 GO-FLOW chart for the RCIC and HPCI.

These two systems have loop structures. The analyses are also performed by using the method to solve loop structure.

GO-FLOW charts are constructed as shown in Fig. 6 for "RCIC and HPCI system". The RCIC and HPCI can be considered as one system with double loop structures, and the chart includes both the RCIC part and HPCI part.

6.3 Core injection by fire pump -Common cause failure-

The system layout is shown in Fig. 4, which is actually taken at the Fukushima Daiichi accident [5]. In the analysis, it is assumed that this system can be started at 5hours after the start of HPCI. Where, the function of HPCI becomes ineffective and the pressure decreases under 2MPa.

If the supply of pure water fails or pure water exhausts, sea water can be used for core cooling. In the analysis of water injection system by fire pump, it also need not consider phased mission condition with the power generation system, RCIC and HPCI.

This "core injection by fire pump" is started in the late stage of accident progression. Temperature and pressure in the containment vessel may abnormally increase because of insufficient cooling. Then, many components are suffered severe conditions and common cause failures will occur. Here, assume all the motor operated valves(MOVs) are suffered common causes. The β-factor method is also used for the estimation of the contribution from common cause failures.

GO-FLOW charts are constructed as shown in Fig. 7. Common cause failures are considered for MOV operating failures (Group1; No.13,30, β=0.3, Group2; No.21,24,25,26, β=0.3) and MOV opening and closing actions (Group3; No.12,27,29, β=0.3).

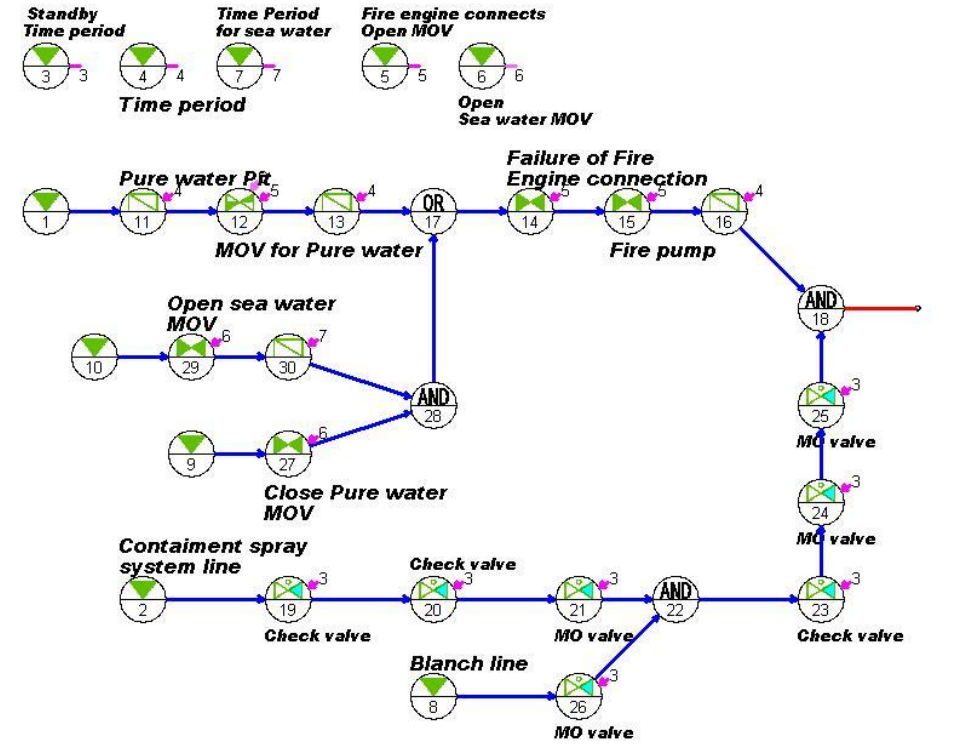

Fig.7 GO-FLOW chart for water injection by fire engine.

6.4 Considerations of human performances

An emergency procedure did not clearly describe the ventilation of containment vessel without electricity and core injection by fire protection pump in case of severe accident. Their actions require “ad hoc” and “flexible” actions. Success probabilities of these actions are strongly dependent on human factors.

Evaluation of human performance is an important issue for the safety analysis of engineering systems, because its errors directly produces malfunction or failure of the systems. To evaluate human error probability is a difficult task. Even for a simple action, its failure probability changes in wide ranges depending on persons characteristics, surrounding working conditions, relation to other tasks, and so on.

Failure probabilities of components in "water injection by fire pump" include human factors. For example, "Fire engine fails to connect", or "MOV failure of open/close action" strongly depend on human performance. But, in the section 6.3, influence of severe and emergency accident condition to human performance is not explicitly considered.

There is an attempt[12] to estimate human performance by a simplified Step Ladder model and the GO-FLOW framework. With the aid of this technique, it is possible to estimate uncertainty and degradation of success probability of the core injection by fire pump. To obtain a specific value of the influence by human performance is future work with the support of more concrete data.

7 Analysis results

Analysis results are shown in Fig. 8. From time 0 hour to time 80 hours, reactor is operated as normal, that is, continues to generate electricity. After 80 hours, the reactor is shut down and the main purpose becomes to cool the reactor core. The missions have been changed.

During the generation of electricity by BWR plant, effect of common cause failure is seen as 11 to 35% increase of mission failure probability

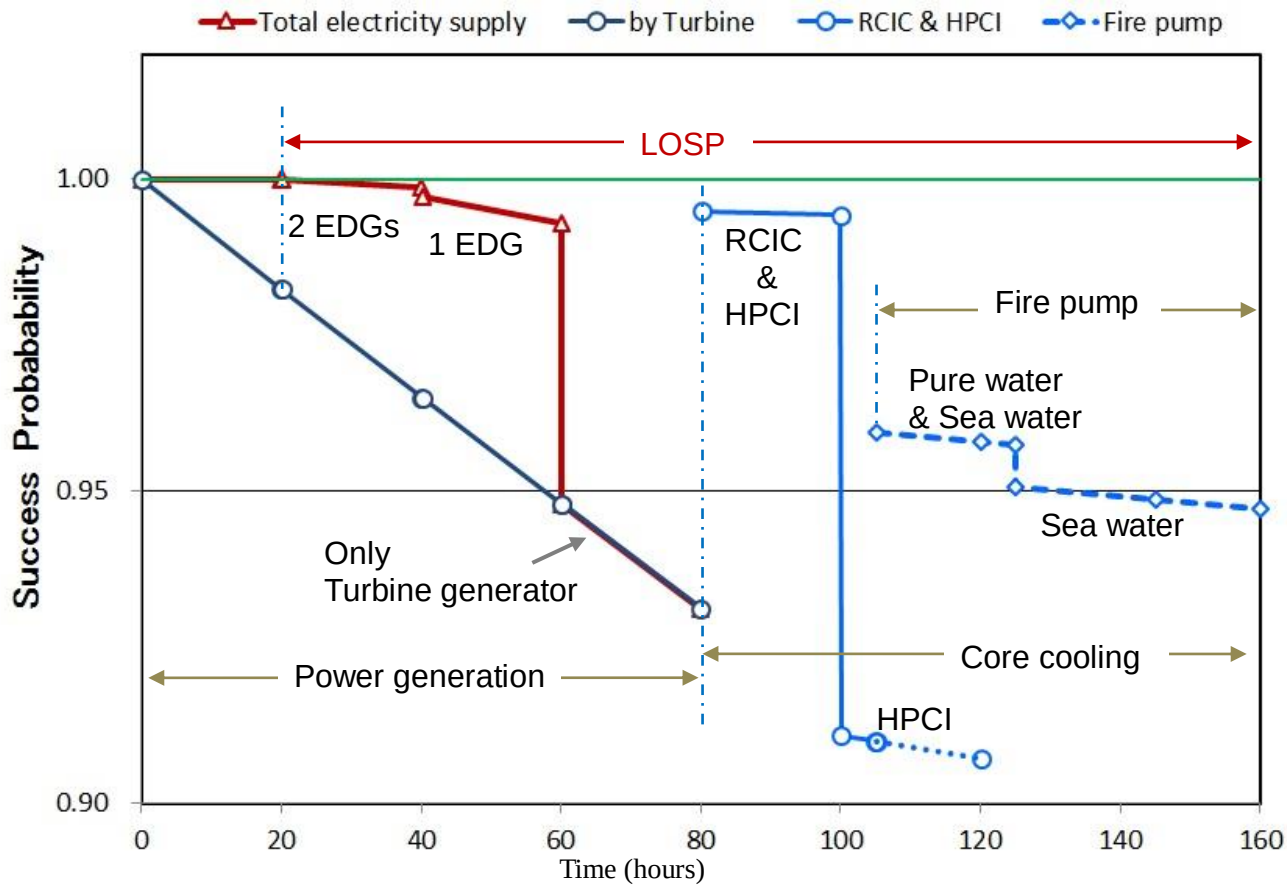

Fig.8 Analysis results.

Success probabilities discontinuously change when operational condition changes. At 80 hours, large increase of success probability is seen but at this point the mission is also changed. Therefore it is no use to make a comparison of the success probabilities before and after the 80 hours.

From RCIC to HPCI, the success probability drastically decreases. This is because of the lost of redundancy by two cooling systems. HPCI cannot continue effective cooling for long time, because of reactor vessel's pressure drop. This situation is indicated by dotted line around 105 to 120 hours in Fig.8.

The water injection by the fire engine is started at 105 hours together with the HPCI operation. The contribution from common cause failure is estimated as the 2% decrease of failure probability from the results without common cause failure. This system is simple and almost the series structure, then common cause failures have positive effects to mission success probability. The success probability is larger than that of HPCI. This is because of simplicity of the system, but the system is emergency and temporal equipment, and possible function is limited. The simple comparison makes misinterpretations

8 Discussions and Conclusions

Mission success probability of nuclear power plant system has been evaluated under accident conditions. Analyses have been made by the GO-FLOW methodology, which is utilized as key technology to the research activity on going at Harbin Engineering University (HEU)[3].

A hypothetical sequence of accident conditions has been settled based on the Fukushima Daiichi accident. Mission success probabilities have been obtained with the growth of accident.

Success probability of system operation, reliability or availability are obtained with some boundary conditions, such as LOSP condition, unavailable equipment, possible resources, and so on. Furthermore, the mission as “power generation” or “core cooling” changes on a progression of accident.

The analysis results as shown in Fig. 8 could be utilized for visualizing risk state intuitively in "risk monitor” system. In this case, boundary conditions of the analysis should be properly presented to persons who are observing risk monitor. A value itself without analysis or boundary conditions would sometimes make misreading.

Uncertainty ranges of mission success probabilities are important information for operators to correspond to accident situation. Uncertainties are produced by failure data distribution, analysis model uncertainty, lack of knowledge and so on. Estimation of uncertainty[13] needs to be performed and shown in "risk monitor" system.

The present analyses have shown that mission success probabilities of nuclear power plant with the growth of accident will be easily obtained by the GO-FLOW methodology.

References

[1] MATSUOKA, T.: Estimation of dynamic behavior of nuclear power plant system state under severe accident conditions, International Journal of Nuclear Safety and Simulation, 2014, 5(3):197-204,.

[2] MATSUOKA, T.: GO-FLOW methodology - Basic concept and integrated analysis framework for its applications, International Journal of Nuclear Safety and Simulation, , 2010, 1(.3): 198-206.

[3] YOSHIKAWA, H., LIND, M., YANG, M., HASHIM, M., and ZHANG, Z.: Configuration of Risk Monitor system by plant defense-in-depth risk monitor and reliability monitor, International Journal of Nuclear Safety and Simulation, 2012, 3(2): 140-152.

[4] MATSUOKA, T.: Evaluation of plant operational states with the consideration of loop structures under accident conditions, Nuclear Engineering and Technology, 2015, 47(2):157-164.

[5] Prime minister of Japan and his cabinet: Report of Japanese Government to the IAEA Ministerial Conference on Nuclear Safety - The Accident at TEPCO's Fukushima Nuclear Power Stations –, June 18, 2011.

[6] Japan atomic energy society: A standard for Procedures of Probabilistic Safety Assessment of Nuclear Power Plants during Power Operation 2008(Level 1 PSA): (AESJ-SC-P008:2008).

[7] IAEA: Survey of ranges of Component reliability data for use in probabilistic safety assessment, IAEA-TECDOC-508,1989.

[8] MATSUOKA, T.; Generalized Method for Solving Logical Loops in Reliability Analysis. In: Proceedings of PSAM-11, Helsinki, Finland, June 25-29, 2012.

[9] MOSLEH, A.: Procedures for analysis of common-cause failures in Probabilistic Safety Analysis, NUREG: CR-5801 SAND91-7087 RG, 4. 1993

[10] HASHIM, M., YOSHIKAWA, H., MATSUOKA, T., and YANG, M.: Common cause failure analysis of PWR containment spray system by GO-FLOW methodology, Nuclear Engineering and Design, 2013, 262: 350-357

[11] MATSUOKA, T., and KOBAYASHI, M.: The GO-FLOW reliability analysis methodology—analysis of common cause failures with uncertainty, Nucl. Eng. Des., 1997,175: 205–214.

[12] MATSUOKA, T., and KATO,Y.: Modeling of a Human Performance by the GO-FLOW Methodology. In: First International Symposium on Socially and Technically Symbiotic Systems, Okayama, August 29-31, 2012,

[13] HASHIM, M., YOSHIKAWA, H., MATSUOKA, T., and YANG, M.: Considerations of uncertainties in evaluating dynamic reliability by GO-FLOW methodology - example study of reliability monitor for PWR safety system in the risk-monitor system, Journal of Nuclear Science and Technology, 2013, 50(7): 695-708.